João Luiz Pereira Marciano

Segurança da Informação - uma abordagem social

Brasília

2006

João Luiz Pereira Marciano

Segurança da Informação - uma abordagem social

Tese apresentada ao Departamento de Ciência da Informação e Documentação da Universidade de Brasília como requisito para a obtenção do título de doutor em Ciência da Informação

Orientador:
Mamede Lima-Marques

CID/FACE-UnB

Brasília

2006

FOLHA DE APROVAÇÃO

Título: Segurança da Informação - uma abordagem social

Autor: João Luiz Pereira Marciano

Área de concentração: Transferência da Informação

Linha de pesquisa: Arquitetura da Informação

Tese submetida à Comissão Examinadora designada pelo Colegiado do Programa de Pós-Graduação em Ciência da Informação do Departamento de Ciência da Informação e Documentação da Universidade de Brasília como requisito parcial para obtenção do título de **Doutor em Ciência da Informação**.

Tese aprovada em: 14/07/2006

Aprovado por:

Prof. Dr. Mamede Lima-Marques
Presidente - Orientador (UnB/PPGCInf)

Prof^a. Dr^a. Marisa Brascher Basílio Medeiros
Membro interno (UnB/PPGCInf)

Prof. Dr. Paulo Carlos Du Pin Calmon
Membro externo (IPOL/UnB)

Prof. Dr. Paulo Henrique Portela de Carvalho
Membro interno (CID/FACE-UnB)

Prof. Dr. Gentil José de Lucena Filho
Membro externo (UCB)

Prof. Dr. Tarcisio Zandonade
Suplente (UnB/PPGCInf)

À memória de
meu pai, Joaquim,
e de meu irmão, Joaquim Luiz.

AGRADECIMENTOS

Agradeço aos amigos e mestres que me ajudaram a trilhar o caminho até aqui.

Resumo

O uso cada vez mais disseminado de sistemas informatizados integrados por meio de redes é um fato determinante da Sociedade da Informação. Este universo de conteúdos e continentes digitais está sujeito a várias ameaças que comprometem seriamente a segurança do complexo usuário-sistema-informação. A tecnologia da informação é capaz de apresentar parte da solução a este problema, mas não é capaz de resolvê-lo integralmente. As políticas de segurança da informação devem contemplar o adequado equilíbrio dos aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos de políticas atuais, extremamente voltados às questões tecnológicas.

Este trabalho teve por finalidade a análise dos pressupostos necessários para o tratamento da segurança da informação, por meio da formulação de políticas de segurança da informação, baseando-se em uma estratégia de análise fenomenológica. Tal abordagem visa a dar às políticas formuladas uma abordagem social, de caráter humanista, centrada nos pontos de vista do usuário e que se contraponha aos modelos tecnicistas atuais.

Para tanto, procedeu-se a uma aprofundada coleta de artigos e trabalhos nas áreas tanto da segurança da informação quanto da formulação e implementação de políticas de caráter público e organizacional, fazendo-se uso de uma análise hermenêutica destes conteúdos. Neste sentido, realizou-se ainda uma tipificação das diferentes abordagens epistemológicas propostas à Ciência da Informação.

Os resultados obtidos sugeriram um modelo para a formulação de políticas de segurança da informação baseadas em moldes afeitos ao domínio das ciências sociais e construídas com ênfase na observação dos sistemas de informação e no contexto em que se inserem.

Palavras-chave

Segurança da informação; políticas de segurança da informação; fenomenologia; hermenêutica; interação social.

Abstract

The ever increasing use of network-integrated information systems is an Information Society's landmark. This universe of digital contents and media is prone to some threats that seriously compromise the security of the user-system-information relationship. Information technology can sugest part of this problem's solution, but cannot solve it integrally. The information security policies must observe the balance between the human and technology issues about information security, in contrast with current policy models, extremely devoted to technological questions.

This work had for purpose the analysis of the required backgrounds for the treatment of the information security, by means of information security policies proposal, based on a strategy of phenomenologic analysis. This approach aims to give to the policies a social boarding, of humanist perspectives, focused in the users's points of view and in opposition to the current technologic models.

For such, the author proceeded to the analysis of a wide collection from articles and works in the fields of information security and public and corporate policies, applying a hermeneutic analysis on these materials. Also, a characterization of the various epistemology approaches to the Information Science was released.

The found results suggested a model for the design of information security policies, based on social sciences requisites and builded with emphasis on the overviewing of information systems and in the context in which they exist.

Keywords

Information security; information security policies; policy networks; phenomenology; hermeneutics; social interaction.

Sumário

Lista de Tabelas

Lista de Figuras

Lista de Siglas

1 Introdução

O uso cada vez mais amplo e disseminado de sistemas informatizados para a realização das mais diversas atividades, com a integração destes sistemas e de suas bases de dados por meio de redes, é um fato determinante da Sociedade da Informação. Contudo, este universo de conteúdos e continentes digitais está sujeito a várias formas de ameaças, físicas ou virtuais, que comprometem seriamente a segurança das pessoas e das informações a elas atinentes, bem como das transações que envolvem o complexo usuário-sistema-informação. A tecnologia da informação é capaz de apresentar parte da solução a este problema, não sendo, contudo, capaz de resolvê-lo integralmente, e até mesmo contribuindo, em alguns casos, para agravá-lo. Nos ambientes organizacionais, a prática voltada à preservação da segurança é orientada pelas assim chamadas políticas de segurança da informação, que devem abranger de forma adequada as mais variadas áreas do contexto organizacional, perpassando os recursos computacionais e de infra-estrutura e logística, além dos recursos humanos. Diante deste panorama, e dada a extrema relevância dos aspectos humanos no contexto da segurança da informação, este trabalho propõe a integração de disciplinas oriundas do âmbito das ciências sociais para a construção de um arcabouço destinado à elaboração, implementação e acompanhamento de políticas de segurança abrangentes, que contemplem com o adequado equilíbrio os aspectos humanos e técnicos da segurança da informação, em contraposição aos modelos atuais, notadamente voltados às questões tecnológicas.

O propósito de advogar para o campo das ciências sociais vários dos temas relativos à segurança da informação advém da observação de que as práticas usuais desta disciplina privilegiam sobretudo os seus aspectos técnicos e tecnológicos, tais como a implementação de ferramentas automatizadas para o monitoramento de diversas atividades dos usuários dos sistemas de informação, sem, no entanto, levar em conta os motivos que levam estes usuários a agir desta ou daquela maneira. Ainda, são comuns as implementações de aplicativos e camadas de software destinadas ao aumento da segurança, como o uso de criptografia, mas que terminam por diminuir acentuadamente a amigabilidade dos sistemas sem, contudo, produzir os resultados esperados. Naturalmente, não se pretende a eliminação de tais ferramentas e aplicativos, mas

sim a adequação de seu uso aos requisitos dos sistemas, portanto aos requisitos dos usuários, aos quais devem atender.

Uma vez que, usualmente, o planejamento das atividades e controles relacionados à segurança da informação no ambiente organizacional, a sua inserção no dia-a-dia da organização e as práticas associadas são tratados no conjunto das assim chamadas políticas de segurança da informação, estas políticas se tornam fundamentais para qualquer enfoque que se pretenda aplicar ao problema. Deste modo, são as políticas, em seus aspectos públicos e organizacionais, o foco escolhido para o desenvolvimento de uma nova abordagem da segurança da informação neste trabalho, conforme se verá nos capítulos seguintes.

Este trabalho propõe que a segurança seja medida por parâmetros intrínsecos à sua própria gênese no contexto organizacional, parâmetros estes que são extraídos do ambiente organizacional e a eles devem ser adequados. Para tanto, propõe-se a ênfase na formulação, formalização e aplicação de políticas da segurança da informação que contemplem tais parâmetros.

Como fundamentos para tal empreitada, além dos subsídios próprios da teoria da informação e da segurança da informação, serão também utilizados conceitos oriundos de disciplinas originárias de diferentes áreas do conhecimento, em busca de indicadores para a correta abordagem dos problemas acima descritos, além de ter-se em vista a categorização que lhes é dada pelas políticas de segurança da informação. Busca-se, deste modo, produzir um todo homogeneamente organizado a partir da correta identificação das partes componentes, cada uma das quais contribuindo com elementos de seu domínio para a solução procurada - respeita-se a percepção de que, uma vez identificados os fatores componentes da problematicidade da segurança da informação, é necessário reportar-se às suas áreas de origem e de excelência para sua devida caracterização e mensuração, além da definição adequada de um roteiro para a solução do problema.

Além da abrangência das políticas, o caráter interdisciplinar da ciência da informação, já muito bem delineado por Saracevic (1995) e por Bates (1999), dentre outros, aponta para algumas das disciplinas que interagem intrinsecamente com esta área. Além da ciência da computação, cujos pressupostos e aplicações não são tratados em detalhes neste trabalho, neste estudo estão contempladas ainda outras áreas do conhecimento, eminentemente a fenomenologia e a hermenêutica, que são as bases epistemológicas para a abordagem do problema, e a ciência política, para o estudo das políticas públicas vistas quanto à sua origem, tipologia e aplicação.

Com o uso de conhecimentos advindos destas áreas, realiza-se a análise da gênese das políticas, dos pressupostos que envolvem esta gênese e do impacto gerado junto aos usuários pela implementação das políticas de segurança da informação nos ambientes organizacionais.

Os objetivos pretendidos com este trabalho e a metodologia empregada são descritos no Capítulo 2.

A fundamentação epistemológica para o trabalho realizado, com o uso de uma abordagem baseada nos conceitos da fenomenologia e da hermenêutica, a fim de proporcionar uma abordagem da segurança da informação sob um enfoque humanista, é mostrada no Capítulo 3.

A contextualização dos conceitos específicos da segurança da informação é vista no Capítulo 4.

As fontes de políticas públicas e organizacionais especificamente voltadas à segurança da informação são analisadas detalhadamente no Capítulo 5.

O arcabouço das ciências sociais confluentes para o tratamento da segurança da informação é mostrado no Capítulo 6.

Os conceitos de políticas e de redes, a gênese das políticas e a sua conformidade ao contexto social do qual advêm e o modelo proposto para a formulação de políticas de segurança da informação de caráter humanista são discutidos no Capítulo 7.

Por fim, a revisão dos passos seguidos à luz da discussão e da metodologia apresentadas, o resumo das contribuições resultantes do trabalho realizado e algumas sugestões para estudos futuros estão no Capítulo 8.

Cumpre ainda ressaltar um outro aspecto deste trabalho: os resultados obtidos estão dispostos de forma esparsa ao longo da apresentação do texto, uma vez que a própria abordagem escolhida apontou como melhor caminho a apresentação de novos conceitos e análises passo a passo com a confecção do texto. Deste modo, cada contribuição proposta pelo autor é apresentada em seu devido contexto, ao lado da concepção vigente e que se pretende discutir.

2 *Objetivo e metodologia*

2.1 Objetivo da pesquisa

ESTE trabalho teve por finalidade a análise dos pressupostos necessários para o tratamento da segurança da informação, por meio da formulação de políticas de segurança da informação, baseando-se em uma estratégia de análise fenomenológica. Tal abordagem visa a dar às políticas formuladas uma abordagem social, de caráter humanista, centrada nos pontos de vista do usuário e que se contraponha aos modelos tecnicistas atuais.

Com vistas a tal finalidade, este trabalho se propôs a seguir os seguintes passos:

1) realizar um amplo levantamento acerca do problema da segurança da informação e de como ele é tratado nos ambientes organizacionais e no ambiente governamental. O resultado deste levantamento é relatado nos Capítulos 4 e 5;

2) fazer uso dos princípios da fenomenologia e da hermenêutica para a descrição de tal problema. Os fundamentos de ambas as teorias estão no Capítulo 3; a descrição do problema tratado concentra-se principalmente nos Capítulos 4 e 5;

3) caracterizar e tipificar as políticas de segurança da informação, apontando as suas origens e os passos para a sua formulação e implementação; esta caracterização encontra-se no Capítulo 5;

4) apontar estratégias alternativas para a elaboração de tais políticas, visando a uma abordagem que se contraponha à usual, tecnicista, complementando-a com aspectos baseados na experiência do usuário frente aos sistemas de informação; esta discussão é apresentada nos Capítulos 6 e 7;

5) apontar complementos e acréscimos à abordagem escolhida para o problema, o que é feito no Capítulo 8.

2.2 Metodologia

A fim de alcançar o objetivo pretendido, foram usados os componentes fundamentais da pesquisa fenomenológica, conforme indicados por Sanders (1982).

Deve-se ressaltar que uma das propostas inicialmente cogitadas foi a da aplicação de instrumentos (questionários e entrevistas) junto aos usuários e gestores de sistemas de informação, com o objetivo de aferir a percepção destes junto ao tema da segurança da informação. Com este objetivo, foi construído um instrumento para a captura desta percepção, apresentado no Apêndice B. Contudo, uma vez procuradas diversas organizações (três públicas e duas privadas) para a aplicação do instrumento, não se obteve resposta afirmativa de nenhuma delas. As respostas alegadas, quando as houve, foram no sentido de que o tema ainda não fora debatido internamente à organização, devendo aguardar-se o "momento adequado" para uma ação da natureza proposta, ou de que a organização passava por um processo interno de avaliação de requisitos relacionados à segurança da informação, e que o pesquisador entrasse em contato posteriormente.

Outra abordagem inicialmente proposta para este trabalho foi a formalização das políticas de segurança da informação por meio de mecanismos da lógica, visando à eliminação de ambigüidades e mesmo ao tratamento computacional das políticas nos ambientes organizacionais. Uma proposta de formalização foi desenvolvida com o uso de lógicas modais e é mostrada no Apêndice C. Porém, algumas questões de cunho anterior à existência das políticas tornaram-se prementes e a elas deu-se destaque, como se verá nas páginas seguintes.

Uma vez que se já realizava uma profunda análise documental de artigos e trabalhos nas áreas tanto da segurança da informação quanto da formulação e implementação de políticas de caráter público e organizacional, foram estes os dados utilizados para a pesquisa. Deve-se ressaltar que a fundamentação de tal abordagem se baseia grandemente na obra de Ricoeur, particularmente (RICOEUR, 1982), onde aquele delineia sua descrição de texto como ação, e, mais especificamente, como uma ação escrita e como um modo legítimo de realização do discurso (RICOEUR, 1982, pp. 13-15,pp. 215ss). Estas acepções serão mais aprofundadas no Capítulo 3.

Antecipadamente, indicam-se os passos propostos para uma pesquisa de caráter fenomenológico, conforme Sanders (1982), e as opções adotadas neste trabalho:

a. **determinar os limites do que e de quem será investigado**: escolheu-se o problema da segurança da informação nos ambientes organizacional e governamental e a solução co-

mumente proposta a ele, qual seja, a formulação e aplicação de regras de conduta, comumente chamadas de políticas de segurança da informação; neste contexto, os indivíduos envolvidos no estudo são os usuários dos sistemas de informação sujeitos aos problemas de segurança da informação analisados;

b. **coletar os dados para análise**: realizou-se uma ampla coleta e análise de relatórios e publicações acerca do tema, caracterizando-se um estudo bibliográfico.

c. **realizar a análise hermenêutica dos dados coletados**: esta análise foi feita ao longo de todo o estudo.

2.2.1 Caracterização da pesquisa

Pelo uso do método de análise fenomenológica, visando a ressaltar propriedades potenciais dos fenômenos observados, as quais usualmente não são analisadas sob um ponto de vista adequado, a pesquisa se caracteriza como eminentemente qualitativa, com aspectos exploratórios (uso de diversas disciplinas para a busca de um modelo de formulação de políticas de segurança da informação, visando ao tratamento adequado dos problemas afeitos à segurança da informação).

2.2.2 Uma nova abordagem para o problema da segurança da informação

A proposta de uma abordagem para as políticas de segurança da informação centrada nos pontos de vista do usuário deve, necessariamente, evitar os conceitos de origem majoritariamente positivista que ora dominam este campo e que lhe dão o caráter essencialmente tecnológico que o caracteriza, ao deixarem em segundo plano o elemento social, como se pode ver em (WOOD, 2002b), (BOSWORTH; KABAY, 2002) e (SCHNEIER, 2000). Assim, a adoção de um modelo interpretativo deve se caracterizar pela desconstrução de boa parte (se não de todos) dos conceitos atualmente em voga na área da segurança da informação e sua posterior reapresentação como componentes de um modelo orientado à visão do homem no contexto informacional em que se insere. Naturalmente, antes de ser apresentado um conceito sob o ponto de vista do novo modelo, deve-se prover seu entendimento sob o *ethos* vigente, bem como deve-se apresentar os motivos para sua desconstrução e as considerações que levaram à sua reconstrução e apresentação sob a nova ótica.

No contexto das ciências, sejam elas sociais ou naturais, os conceitos essenciais à formulação de um modelo são apresentados na forma de construtos, ou seja, elementos essenciais que

dão identidade ao modelo, dentre os quais devem ser ressaltados aqueles que o levam a diferir dos demais modelos existentes. Contudo, é preciso diferenciar os construtos utilizados no modelo e que são apresentados pela própria existência do tema em tratamento, tais como, no caso da formulação de políticas de segurança da informação, os construtos "sistema de informação", "segurança da informação", "informação‘‘, "política de segurança" e "usuários", aqui chamados para efeitos de simplificação de construtos de primeiro nível, dos construtos utilizados para a apresentação do modelo em si, tais como a metodologia e os métodos utilizados na construção e descrição do modelo, aqui chamados de construtos de segundo nível. Uma vez que se apresenta um novo modelo para o tratamento do problema da segurança por meio das políticas de segurança da informação, cuja descrição é dependente da abordagem considerada, retarda-se por ora a apresentação dos construtos de primeiro nível, sendo agora apresentados os construtos de segundo nível.

A delimitação do campo de conhecimento abordado por um modelo (o qual pode vir, *a posteriori*, a se configurar em uma teoria [1] e que é, desde sempre, suscetível à falibilidade e a refinamentos) é determinada, primeiramente, pela *ontologia*, ou seja, pelo estudo da existência e das propriedades, do "ser enquanto ser", do objeto considerado. A cada ontologia, por sua vez, pode-se aplicar diversas formas de representação e análise do conhecimento ali considerado, caracterizando-se diferentes visões de um mesmo objeto de estudo. Esta análise cabe à *epistemologia*, por vezes identificada como o estudo dos resultados das ciências, com aplicações finalísticas em campos diversos, mas que aqui é entendida como um questionamento de origem eminentemente filosófica acerca da própria natureza do conhecimento, e por extensão das ciências, e que versa sobre as justificativas da verificabilidade do conhecimento adquirido ou acumulado. Em outras palavras, a epistemologia encarrega-se de avaliar os critérios de verificabilidade das asserções trazidas à luz pela ontologia em uso, no processo conhecido como *verificação epistêmica*. Desta forma, diferentes epistemologias podem ser aplicadas a uma mesma ontologia, sendo que várias epistemologias têm sido desenvolvidas e aplicadas em diferentes contextos históricos e sócio-econômicos, tais como o racionalismo e o existencialismo. A seção 3.1 apresenta diversas abordagens epistemológicas que têm sido aplicadas especificamente à ciência da informação.

Eis aí a diferença essencial entre as ciências sociais e as ciências naturais: enquanto nestas o conhecimento é apresentado sob a forma da verificabilidade repetitiva de fenômenos observáveis, no processo delineado pelo modelo galilaico-cartesiano, naquelas o conhecimento se

[1] Segundo Popper, uma teoria é caracterizada por quatro propriedades: consistência lógica interna, testabilidade empírica, robustez a falhas empíricas (deve ser capaz de suportar os "falsos positivos" e os "falsos negativos") e ser tão explicativa ou preditiva quanto qualquer outra teoria com a qual rivalize (LEE, 2004).

estabelece sob a forma de interpretações e asserções acerca de fatos e objetos concretos ou abstratos, em um processo cujas origens remontam ao ciclo plato-socrático e que estabelece a fundamental importância, para a epistemologia, da interpretação adotada pelo observador. A análise destas interpretações é o papel da *hermenêutica*, que tendo surgido voltada para a análise de textos sagrados, ampliou sua abrangência para todas as áreas do conhecimento. A pergunta essencial à qual a hermenêutica se propõe a responder é: dado o conjunto de pressupostos aos quais todos os indivíduos estão sujeitos - pressupostos estes oriundos da visão de mundo particular a cada um - como se pode garantir que determinado conhecimento é correto, ou seja, que ele é verificável independentemente dos pressupostos individuais? Deve-se salientar que a própria questão distancia-se diametralmente do modo positivista de ciência, o qual pressupõe que o cientista "ponha de lado" a sua subjetividade, principalmente o positivismo indutivo, voltado a generalizações a partir de exemplos obtidos de amostras nem sempre representativas, mas que se mostra alheio ao problema apontado por Hume (LEE, 2004), qual seja, o da própria inexeqüibilidade de generalizações por meio do processo indutivo.

Um dos grandes teóricos da hermenêutica, Hans-Georg Gadamer, apresentou uma solução assaz instigante para esta questão: a fim de se garantir a veracidade de uma interpretação, deve-se, primeiro, assumir-se a existência dos pressupostos existentes, e em seguida proceder-se a uma avaliação destes pressupostos à luz da epistemologia considerada (GADAMER, 1998; ALCOFF, 1998). Dois dos pressupostos que Gadamer apresenta como onipresentes a todas as interpretações são a autoridade e a tradição. Como se verá, tanto uma como a outra, quanto à segurança da informação e especificamente quanto às políticas, serão questionadas continuamente ao longo deste trabalho. Antecipe-se ainda que os trabalhos de Martin Heiddeger (HEIDEGGER, 1985) e de Paul Ricoeur (PETIT, 2003; VILLELA-PETIT, 2003) são utilizados como pano de fundo para a execução de uma hermenêutica dos temas atinentes à segurança da informação.

Uma vez estabelecido o campo do conhecimento e delineado o enfoque a ser aplicado para a sua verificabilidade, procede-se à determinação das *metodologias* que serão utilizadas para a construção do modelo. Uma metodologia corresponde a um conjunto coeso e coerente de *métodos*, ou seja, técnicas ("know-how") que deverão orientar a observação dos fenômenos de interesse e conduzir a análise dos dados colhidos acerca de tais observações. Ao longo deste trabalho será proposta não apenas uma, mas um conjunto de variadas metodologias, constituindo o que se compreende por multimetodologia - em cada etapa do processo construtivo do modelo, empregar-se-á uma metodologia para a sua consecução.

Este processo de construção de um modelo de conhecimento pode ser representado pela

Figura 1. Ali, ilustra-se o fato de que cada um dos níveis superiores pode ser analisado ou implementado sob a ótica de um ou vários dos componentes do nível imediatamente inferior.
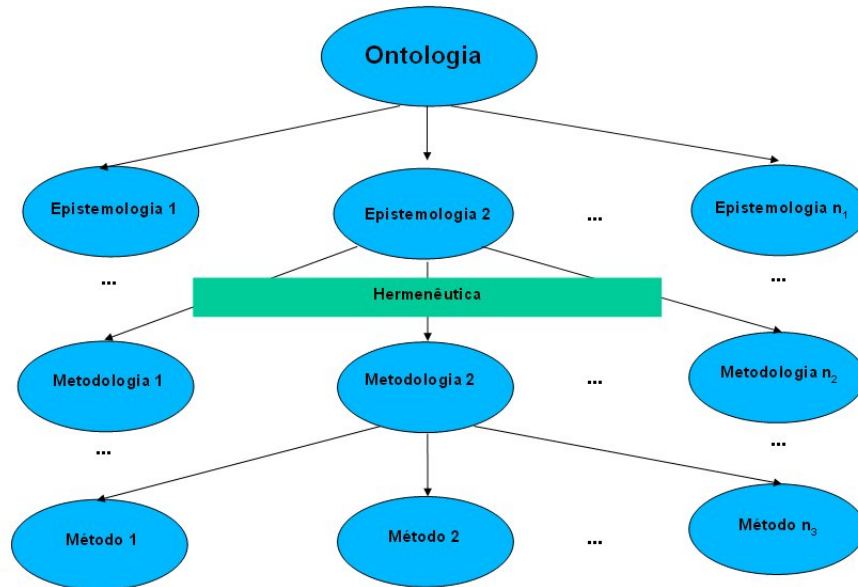
Figura 1: Hierarquia para a construção de modelos conceituais do conhecimento.

No presente trabalho, a epistemologia escolhida para a construção do modelo proposto é a *fenomenologia*, por ser uma dentre as correntes filosóficas que se encarregam de analisar o significado das interações sociais e das ações individuais. Mais particularmente, a escolha recaiu sobre esta escola por sua visão *sui generis* do processo de formação do conhecimento e da validação de sua veracidade.

Por ora, adiante-se que a fenomenologia, como seu nome indica, enxerga o conhecimento sob a ótica dos fenômenos, ou seja, acontecimentos que se processam no mundo e que são analisados por um observador inicialmente imbuído de uma atitude natural, isto é, passiva, em relação a tais fenômenos. No momento em que se dedica a considerá-los de forma mais detida, especificamente sob o ponto de vista filosófico, ou seja, quando leva em consideração a gênese, estrutura e finalidade de tais fenômenos, o indivíduo adota uma nova postura, a chamada atitude filosófica, a qual se caracteriza, segundo a fenomenologia, pela observação das "coisas mesmas", ou seja, em sua essência. Neste processo, o observador apreende do objeto de observação as características conformadoras de sua essência, formando em sua mente uma imagem do objeto analisado. O sentido do que se percebe depende de como isto é subjetivamente experienciado - princípios e fatos são mediados pela experiência tanto pregressa quanto atual do observador. Na atitude filosófica, segundo Janicaud (2000), os únicos pré-julgamentos dos quais o indivíduo deve se abster são aqueles doxásticos, ou seja, relacionados a eventuais

obrigações, deveres e proibições quanto à tradição ou às teorias ou propostas que acaso deseje defender.

Para verificação do conhecimento apreendido, o critério de veracidade aplicado pela fenomenologia é a coerência entre a imagem formulada e o objeto. Está-se, deste modo, diante de uma tríade de domínios do conhecimento:

- a **ontologia**, ou ciência própria ao campo de conhecimento, que se ocupa da análise do objeto, ao descrever suas propriedades e elementos essenciais;
- a **psicologia**, que se ocupa da análise do sujeito frente a seu ambiente e do processo de formulação do seu raciocínio; e
- a **lógica**, que se ocupa da verificação da adequação entre o objeto e a imagem construída no processo de apreensão do conhecimento.

Desta forma, uma vez que se propõe uma abordagem do problema da segurança da informação sob o ponto de vista dos usuários, precisa-se de uma teoria social na qual devem se basear as considerações de caráter sociológico ou grupal sobre as quais se fundamenta a análise realizada. A teoria social adotada neste trabalho é a do interacionismo simbólico, discutida no Capítulo 6. Quanto a uma teoria psicológica, na qual devem se basear as considerações de caráter individual concernentes à interação do indivíduo com a informação e com a sua segurança, foram feitos ensaios, mostrados no Apêndice A, devendo se salientar ainda que, por ocasião da qualificação do doutorado, a banca examinadora optou por recomendar que fosse dada ênfase aos aspectos epistemológicos do trabalho, deixando a aplicação do instrumento e as demais questões afeitas à abordagem da Psicologia para estudos posteriores.

Por seu turno, embora as definições apresentadas por Shannon (1948) e Shannon e Weaver (1975), tais como a de informação como medida da entropia ou quantidade de energia de um sistema, sejam voltadas muito mais a aplicações destinadas à mensuração do volume informacional envolvido em uma troca de mensagens que à compreensão em si dos fenômenos pelos quais a informação é gerada ou transferida, são apresentados ali três questionamentos de fundamental importância para a compreensão destes fenômenos:

- com que exatidão pode-se transmitir símbolos de comunicação (o chamado problema técnico da teoria da informação);
- com que precisão os símbolos transmitem o significado desejado (problema semântico);

- com que eficiência o significado recebido afeta o comportamento do receptor (problema da eficiência).

O esquema clássico elaborado por Shannon (1948), com uma atualização devida ao contexto tecnológico atual, é ilustrado pela Figura 2.
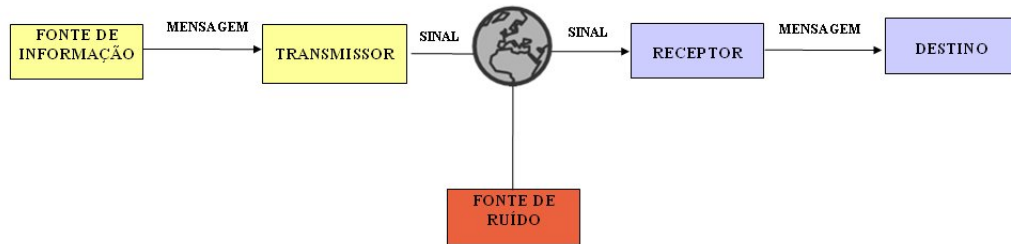
Figura 2: Esquema do sistema emissor-canal-receptor (Adaptado de Shannon (1948)).

O chamado problema técnico, como salienta sua própria denominação, está afeito às áreas de tecnologia. Resta, assim, a uma abordagem social da informação, deliberar acerca dos dois problemas subseqüentes. Neste trabalho, o problema semântico foi abordado sob a ótica de uma identificação adequada, do ponto de vista do usuário, dos principais conceitos envolvidos (ontologia), enquanto o problema da eficiência foi enquadrado sob a ótica da formulação de políticas, atualmente a principal alternativa estratégica para o tratamento dos problemas da segurança da informação (vista sob a égide do interacionismo simbólico).

3 Fundamentos epistemológicos, fenomenologia e hermenêutica

COMO CIÊNCIA multidisciplinar, a ciência da informação permeia diversas áreas, sendo por elas influenciada e ainda carecendo de sólidos fundamentos epistemológicos. A análise dos problemas relacionados ao ciclo da informação é feita de modo multifacetado e fragmentado, com o uso de diversos métodos e metodologias que muitas vezes falham ao se reportar à sua base epistemológica e que ilustram uma dependência intrínseca, mesmo que involuntária, quanto às preferências pessoais ou coletivas dos autores, preferências estas que nem sempre são claramente expostas. A fim de elucidar o campo epistemológico com o qual lida a ciência da informação e para justificar a escolha feita na confecção deste trabalho, apresentam-se a seguir algumas das abordagens apontadas na literatura.

3.1 Abordagens epistemológicas à ciência da informação

Uma edição especial do *Journal of Documentation* (v. 61, n. 1 - 2005), intitulada *LIS and the philosophy of science* [1] traz diversos artigos acerca das diferentes abordagens pelas quais a ciência da informação pode ser tratada, sob o ponto de vista epistemológico. Estes artigos estão citados na Tabela 1, juntamente com uma análise sucinta sobre cada um deles.

[1] *LIS=Library and Information Science*.

Tabela 1: Epistemologias aplicadas à ciência da informação.

Referência	Comentário
Hjørland (2005c)	Introduz a edição com a seguinte sentença : "na comunidade de ciência da informação o interesse pela filosofia da ciência tem sido muito limitado, com exceções a esta tendência geral".
Wikgren (2005)	Propõe o **realismo crítico**, baseado em Bhaskar, como uma abordagem filosófica e como teoria social para a ciência da informação; ressalta a diferenciação entre ontologia e epistemologia. Mingers (2004b) e Mingers (2004a) também apresentam o realismo crítico como alternativa a abordagens positivas e interpretativas, citando especificamente, neste último caso, a metodologia SSM (*Soft Systems Methodology*). Contudo, há severas críticas quanto à fundamentação ontológica e epistemológica do realismo crítico e a seu tratamento, considerado eminentemente causal, ao paradigma interpretativo (KLEIN, 2004).
Sundin e Johannisson (2005)	Aponta o **neo-pragmatismo**, baseado em Rorty, associado a uma perspectiva sociocultural baseada no pedagogia de Vygotsky, com o foco analítico sobre as ações pessoais manifestas e suportadas por ferramentas físico-lingüísticas, como um modelo epistemológico para estudos de necessidade, busca e uso da informação, apontando alguns trabalhos realizados por diversos autores. Hjørland (2004) salienta que esta perspectiva se contrasta ao individualismo epistemológico, mas ressalta a necessidade de melhor fundamentação filosófica para este arcabouço. Hansson (2005) (vide abaixo) questiona ainda o valor científico da postura neo-pragmática.
Budd (2005)	Examina a aplicação de métodos baseados na **fenomenologia** a estudos informacionais, citando conceitos e formulações de Husserl, Heidegger e Merleau-Ponty, entre outros. Salienta a hermenêutica como interpretação aplicada, citando o pensamento de Ricoeur. Estes autores e conceitos serão discutidos nas próximas seções.

continua na próxima página

Referência	Comentário
Radford e Radford (2005)	Apresenta as raízes do **estruturalismo** e do **pós-estruturalismo**, com base em de Saussure e Foucault. Sugere que o foco de atenção de tais epistemologias, ou seja, os princípios de organização de um sistema de linguagem por meio da identificação de padrões existentes nas estruturas lingüísticas, sejam utilizados para base do planejamento e organização de acervos documentários.
Talja, Tuominen e Savolainen (2005)	Descreve as premissas básicas do **construtivismo social** (Piaget, Kelly e Vygotsky), com o conceito de que os processos mentais de construção da realidade relacionada ao mundo são sensivelmente influenciados por convenções sociais e pelas interações vividas pelo sujeito com indivíduos e grupos significantes; a mudança da unidade de estudo do nível individual para o nível social, organizacional e de comunidades de interesse é nomeada pelos autores como **coletivismo**; ainda, o artigo trata do **construcionismo** (Volosinov, Bakhtin, Wittgenstein, Foucault e Garfinkel), com sua ênfase no discurso como o meio pelo qual o indivíduo e o mundo são articulados. O próprio artigo apresenta críticas a cada uma destas abordagens, concluindo que são abordagens complementares. A utilização deste complexo de epistemologias em um único estudo apresenta-se como extremamente complexa, demandando o domínio e a inter-relação de uma variedade de "ismos", como sugere o próprio título do artigo.
Hansson (2005)	Apresenta a **hermenêutica** (Ricoeur) como conexão entre o moderno e o pós-moderno na ciência da informação. Aponta para o aumento no número de trabalhos que utilizam esta abordagem, e salienta que uma ampla gama de problemas tratados na ciência da informação são de natureza interpretativa. A análise hermenêutica é objeto da seção 3.4.

continua na próxima página

Referência	Comentário
Seldén (2005)	Realiza uma análise crítica da ***Grounded Theory*** (Glaser e Strauss), baseada amplamente em métodos empíricos e com profundas raízes no interacionismo simbólico e no positivismo estatístico, apresentando-a como uma possível ferramenta para a formulação de teorias no campo da ciência da informação. A coleta de dados em campo é requisito fundamental para a sua aplicação.
Hjørland (2005b)	Apresenta um breve histórico do **empiricismo** (Locke, Berkeley, Hume, Stuart Mill), do **racionalismo** (Descartes, Spinoza e Leibniz), do **positivismo** (Comte) e do **positivismo lógico** (Frege, Quine, Wittgenstein), citando trabalhos influenciados por tais epistemologias e problemas que podem ser abordados por elas, como a consistência na indexação de documentos e a pesquisa de relevância na recuperação de informações.
Hjørland (2005a)	Sumariza os artigos anteriores e cita o **ecleticismo**, com o uso em um mesmo estudo de abordagens diferentes e talvez conflitantes, ressalvando a suscetibilidade a críticas quanto à fundamentação e à aplicabilidade de tal abordagem.

Percebe-se uma grande variedade de possíveis epistemologias, não por coincidência em grande parte derivadas da filosofia da linguagem, sendo algumas conflitantes, que podem ser utilizadas em estudos da ciência da informação. Se, por um lado, isto corrobora em termos basilares a interdisciplinaridade atribuída a esta ciência, uma vez que lhe dá maleabilidade na escolha das ferramentas e recursos a serem utilizados, capacitando-a a imiscuir-se entre diversos domínios fornecendo-lhes e deles obtendo suporte instrumental, por outro indica claramente a necessidade de uma melhor fundamentação desta ciência sobre alicerces mais estáveis. Ao lado deste debate epistemológico, ocorre um outro pelo viés filosófico-ontológico, onde os filósofos e os teóricos dos fundamentos da ciência da informação visam a identificar e caracterizar claramente as próprias bases filosóficas desta ciência.

Neste sentido, Floridi (2002b, 2003b) tenta delimitar o campo dos estudos filosóficos acerca da informação, iniciando por contextualizá-los historicamente, caracterizando-os como um novo campo e sugerindo que sejam abarcados pela expressão “filosofia da informação”, definida por aquele autor nos seguintes termos:

> Filosofia da informação é o campo filosófico que se dedica a: a) investigação crítica da natureza conceitual e dos princípios básicos da informação, incluindo sua dinâmica, utilização e ciências, e b) elaboração e aplicação de metodologias teóricas e computacionais da informação a problemas filosóficos (FLORIDI, 2002b, p. 137).

A dinâmica da informação apontada na primeira parte da definição acima diz respeito à constituição e modelagem de ambientes de informação, ao ciclo da informação e à computação, tanto algorítmica quanto processual, privilegiando a informação sobre a computação, uma vez que esta não subsiste sem a pressuposição daquela. A segunda parte da definição, por sua vez, indica que a filosofia da informação agrega os requisitos de uma metodologia, voltada a dar suporte aos estudos da Filosofia no que tange aos temas da informação. Em ambos os sentidos, a filosofia da informação lida com três tipos de domínios: tópicos (fatos, dados, problemas, fenômenos, observações), métodos (técnicas, abordagens) e teorias (hipóteses, explanações), visando a analisar diversos problemas (Floridi (2004b) aponta dezoito deles) nos campos da análise, semântica e na própria natureza da informação (o que ela é e como se forma, por exemplo). Duas abordagens à filosofia da informação são apontadas em Floridi (2003a), uma analítica, voltada aos problemas conceituais e à lacuna de conceitos decorrentes da avalanche informacional experimentada nos últimos tempos, e outra metafísica, dedicada à inserção e à reinterpretação do Eu perante o mundo em transformação, construído virtualmente a partir de conceitos outrora eminentemente físicos. Outros conceitos relacionadas à filosofia da informação, alguns aderentes à visão de Floridi, outros complementares, como a aplicação dos conceitos de Shannon (teoria da informação) e Wiener (cibernética) em uma abordagem mais pragmática aos problemas filosóficos da mente e da formação de significados (ADAMS, 2003), estão disponíveis, dentre outras fontes, em dois números especiais do periódico *Minds and Machines* (v. 13 n. 4 - Nov. 2003 e v. 14 n. 1 - Fev. 2004).

Também muito relevante à discussão acerca dos fundamentos epistemológicos da ciência da informação e da interação entre filosofia e informação é o número especial de um outro periódico, *Library Trends - LIS and philosophy (v. 52 - n. 3 - 2004)* - a incidência de artigos e particularmente de números especiais de periódicos de primeira linha acerca destes temas mostra a sua efervescência. Deste último periódico, dois artigos merecem consideração especial para a discussão tratada neste capítulo. No primeiro deles, Cornelius (2004) questiona os argumentos de Floridi (2002a) tanto acerca de que a ciência da informação seja filosofia da informação aplicada quanto o conceito de filosofia da informação apresentado por Floridi, que Cornelius considera “inocente acerca do caráter social” cumprido pela ciência da informação e dissociada dos aspectos práticos da área. No segundo artigo, Floridi (2004a) reafirma suas asserções, alegando que os aspectos práticos da ciência da informação não prescindem de uma

embasada fundamentação teórica, ao mesmo tempo em que a avaliação dos conceitos acerca da informação em moldes filosóficos não exclui a aplicação de métodos e metodologias em estudos informacionais. Particularmente, Floridi considera tediosa a discussão sobre "o que é a informação", por não haver uma maneira simples de resolvê-la, preferindo considerar a questão "onde a informação está" - na mente ou no mundo? Em sua concepção, a informação encontra-se na interface entre o homem o ambiente, como um limiar entre estes dois espaços - uma visão, de resto, claramente fenomenológica.

O debate acerca dos fundamentos da informação está longe de terminar. Na verdade, mal parece ter se iniciado. Para os fins deste trabalho, visando à adoção de uma abordagem humanista e social para os problemas da segurança da informação e tendo em vista os argumentos apresentados pelos autores acima citados e os próprios estudos e propostas já realizados, como a sugestão feita por Wilson (2003) de empregar-se a fenomenologia como arcabouço de integração dos estudos da informação, adotou-se uma postura fenomenológica, cujos conceitos e métodos serão apresentados a seguir.

3.2 As bases da teoria fenomenológica

3.2.1 Husserl

A fenomenologia representa uma dentre as diversas correntes filosóficas que se sedimentaram no decorrer do século XX, especialmente em sua primeira metade. Naquele período, as principais inquirições, conjeturas e publicações sobre o tema são devidas a Husserl e aos dois maiores expoentes existencialistas da Fenomenologia, Heidegger e Merleau-Ponty.

Edmund Husserl (1859-1938) preocupa-se com a perfeita caracterização do estado da mente consciente, identificado por ele como o elemento principal do ser, numa clara alusão à máxima cartesiana: "Penso, logo existo" (HUSSERL, 1996). Com este objetivo, Husserl propõe rejeitar-se a aparente realidade do mundo (o conjunto das entidades físicas e perceptíveis), colocando-o "entre parênteses" (*Einklammerung*), método por ele denominado *epoché* fenomenológica (LÜBCKE, 1999): uma vez que o mundo e todas as suas entidades estão sempre presentes, quer sejam ou não experienciadas pelo observador, ele (o mundo) não deve interferir no processo de formulação do raciocínio, o qual, por sua vez, determina a realização da consciência. O que resta, após este processo de distanciamento, é o *self* que experimenta o mundo, estando a ele conectado pelo que Husserl chama de Ego Transcendental, o qual fornece razão e significado ao mundo e que existe independentemente da existência deste (MINGERS, 2001b).

Para Husserl, o processo de indução fenomenológica compreende as seguintes etapas (HUSSERL, 1996; FRAGATA, 1959; SANDERS, 1982):

1. a análise "intencional" da relação entre o objeto como é percebido (*noema*) e a sua apreensão subjetiva (*noesis*); Husserl cunhou o termo "intencional" para representar a relação entre o objeto e sua aparência junto à consciência que o percebe, ou seja, seu significado;

2. a *epoché*, conforme descrita anteriormente;

3. a redução eidética (*eidos* = essência), o processo pelo qual se abstraem essências a partir da consciência e/ou da experiência, indo além dos padrões e estruturas convencionais de pensamento e ação a fim de identificar suas raízes comuns.

Deste modo, para Husserl o conhecimento não reside no observador nem tampouco no objeto observado, mas na concepção ou imagem do objeto formulada pelo observador. Husserl define a verdade como sendo a concordância perfeita entre o significado (formulado pelo observador) e o que é dado (o objeto), contextualizando o conhecimento como mais um dos fenômenos de estudo vistos por meio da *epoché* (STEGMÜLLER, 1977, p. 58-91).

Com esta formulação, Husserl influenciou grandemente a moderna teoria da consciência, com profundo impacto em ciências como a sociologia (PAUL, 2001; DAVIS, 1997; MYLES, 2004), a psicologia tanto clínica (CAIRNS, 2002; SKRAPEC, 2001; BURKITT, 2003) como organizacional (SCHABRACQ; COOPER, 1998; KARLSSON; CHRISTIANSON, 2003) e a administração (WHITE, 1990). Além disso, até o final de sua vida procurou manter uma postura crítica, mas equilibrada, acerca da ciência e da sua aplicação e desenvolvimento (HUSSERL, 1970).

De modo sucinto, segundo Sanders (1982) a pesquisa fenomenológica baseia-se em quatro grandes questões:

1. como o fenômeno ou experiência sob investigação pode ser descrito?

2. quais são os invariantes ou comunalidades, ou seja, os elementos comuns ou temas emergentes em tais descrições?

3. quais as possíveis reflexões acerca destes temas?

4. quais são as essências presentes nestes temas e reflexões?

Claramente, a fenomenologia se debruça sobre questões filosóficas envolvidas na geração do conhecimento e em sua aplicação, além de apresentar-se como uma epistemologia amplamente afeita a análises de fenômenos sociais e humanos. Neste particular, a própria sociologia tem adotado a abordagem fenomenológica em contrapartida à abordagem clássico-científica ou normativa, no dizer de Wilson (1970), a qual se baseia na formulação e verificação de hipóteses.

A Tabela 2 apresenta as distinções apontadas por Sanders (1982) entre os paradigmas fenomenológico e normativo.

Paradigma fenomenológico	Paradigma normativo
1.Apreensão do mundo	
O pesquisador enxerga o mundo como indeterminado e problemático. Os fenômenos sob investigação são vistos mais diretamente como resultantes de percepções, intuição e significados pessoais.	O pesquisador vê o mundo como aproximadamente determinado ou não problemático. Escolhas pessoais ainda são necessárias para decidir quais características devem ser estudadas e como devem ser avaliadas.
2. Fenômenos investigados	
Considera-se a "experiência vivida" pelos indivíduos. Considera tanto as características observadas como as qualidades específicas percebidas como formas pessoais de significado.	Considera as características que são facilmente enumeráveis e empiricamente verificáveis.
3. Formulação do problema	
Inicia-se com uma atitude de *epoché*. Todos os preconceitos pessoais, crenças e afirmações sobre relações causais ou suposições são suspensas ou "colocadas entre parênteses". Questões são formuladas e as respostas são analisadas.	Inicia-se com uma hipótese de relação causal. A hipótese é verificada pela manipulação de uma ou mais variáveis independentes a fim de estudar-se o seu efeito sobre um comportamento específico (variável dependente).
4. Metodologia de pesquisa	
Dá-se ênfase à descrição do mundo pelo ponto de vista das pessoas que o vivem e o experienciam. Todos os conceitos e teorias emergem dos dados da consciência, exigindo uma abordagem cognitiva que não pode ser replicada com exatidão.	Amplas generalizações abstratas ou teorias são aplicadas de uma forma lógico-dedutiva por meio das hipóteses das definições operacionais para formar um delineamento que pode ser replicado.
5. Objetivo e inferências da pesquisa	
Chegar a essências universais puras. A lógica da inferência é a comparação direta, resultando em novos *insights* ou reclassificações.	Interpretação estatística dos dados a fim de formular categorias ou normas. A lógica da inferência é a classificação e a serialização dos resultados, levando a comparações numéricas.
6. Generalização dos resultados	
As generalizações dizem respeito apenas aos indivíduos específicos sob investigação. As conclusões servem como uma base de dados para investigações posteriores.	Generalizações são feitas com base na análise dos dados relativos a classes similares ou tendências universais que são expressas de um modo normativo (causa/conseqüência, situação/ação, correlação).

Tabela 2: Contrastes entre os paradigmas de pesquisa fenomenológico e normativo (adaptada de Sanders (1982, p. 358)).

3.2.2 Heidegger

Martin Heidegger (1889-1976), para quem "um fenômeno é o que se mostra em si mesmo" (HEIDEGGER, 1985, p. 58), extendeu ainda mais os limites da Fenomenologia. Enquanto Husserl entende a cognição como pensamento puro, Heidegger a vê como uma ação engajada, ao intuir que o homem, como ente auto-consciente, tem seu modo de ser caracterizado exatamente

por sua forma de experimentar o mundo (HEIDEGGER, 1998; MINGERS, 2001b; CROWELL, 2002). Em sua maior obra, *Ser e Tempo*, Heidegger delineia o que ele chama *Dasein*, traduzido como pré-sença (HEIDEGGER, 2002) ou ser-no-mundo (GEORGE, 2000), deixando clara sua preocupação com o ser humano como coletividade e não mais como indivíduo - sua preocupação, assim, não se restringe ao ser humano, mas abarca o Ser consciente e inserido no mundo. Para Heidegger (1943), a essência da verdade consiste na liberdade de ser completo, ser e deixar ser.

A influência do pensamento de Heidegger estende-se desde a medicina e a enfermagem (DRAUCKER, 1999; SADALA; ADORNO, 2002; THORNTON; WHITE, 1999) até os sistemas de informação, sendo vista na obra de diversos autores. Particularmente, suas discussões sobre a linguagem e a comunicação levaram à formulação de conceitos fundamentais, tais como (MINGERS, 2001b):

- a cognição e o pensamento não são funções mentais isoladas; fazem, isto sim, parte das atividades do dia-a-dia, tornando-se essenciais ao ser-no-mundo;
- o conhecimento não consiste de representações de entidades objetivas independentes, formadas nas mentes dos indivíduos; ao invés disso, cada indivíduo realiza distinções, pelo uso da linguagem, no curso de suas interações com outros indivíduos, numa estruturação e reestruturação contínuas do mundo;
- a comunicação trocada em tais interações baseia-se na tradição e nas experiências pregressas, num complexo histórico dos agrupamentos estruturais formulados pelos indivíduos;
- a linguagem é a mais importante dimensão das ações do homem, mas ela deve ser vista como uma ação social por meio da qual o homem coordena suas atividades, mais que meramente como um veículo representativo e denotacional.

A influência de Heidegger é ainda maior ao se tratar sobre os estudos hermenêuticos do comportamento, conforme se verá mais adiante, na seção 3.4.

3.2.3 Merleau-Ponty

Maurice Merleau-Ponty (1908-1961) tem como uma de suas principais obras "Fenomenologia da Percepção" (MERLEAU-PONTY, 1971), em cujo prefácio ele define a fenomenologia como sendo um movimento bidirecional: é ao mesmo tempo um desapegar-se do mundo e um retornar a ele. Merleau-Ponty se preocupa principalmente com a natureza da reflexão filosófica

(HEINÄMAA, 1999). Para ele, nem o mundo determina a percepção nem a percepção constitui o mundo. A cognição está inserida no corpo e no sistema nervoso do homem, dele sendo uma parte intrínseca - além disso, percepção e ação estão mutuamente ligadas, uma vez que percepções envolvem ações motoras e ações geram novas percepções (MINGERS, 2001b).

Também fundamental em Merleau-Ponty é o conceito de *Embodiment* ("a forma real e as capacidades inatas do corpo humano" (DREYFUS, 1996)), retomado por autores como Varela, Thompson e Rosch (1993) em sua teoria da cognição atuante (*enactive cognition*), cujos dois principais aspectos são (MINGERS, 2001b):

- a percepção consiste de ações guiadas de forma perceptiva (ou seja, a percepção de fatos anteriores influencia a percepção de fatos subseqüentes); e
- novas estruturas cognitivas emergem dos padrões senso-motores que permitem à ação ser guiada pela percepção.

Deste modo, a atividade do organismo condiciona o que pode ser percebido num ambiente, e estas percepções, por sua vez, condicionam ações futuras. Deve-se acrescentar ainda que Merleau-Ponty integrou a análise fenomenológica à psicologia e à neurologia antes que uma definição formal das ciências cognitivas fosse apresentada como abarcando estas duas ciências (GALLAGHER; VARELA, 2001), numa associação que se vê cada vez mais aprofundada (BRUZINA, 2004; GODFREY-SMITH, 2001), além de serem vistas grandes afinidades entre os suas obras e as de outros autores sociais, como Searle e Bourdieu (MARCOULATOS, 2001, 2003).

3.3 Ciência da Informação e Fenomenologia

A interconexão entre a Fenomenologia e a Ciência da Informação mostra-se ainda mais evidente quando se observa que a primeira conceitua a linguagem como origem e expressão do conhecimento, ao passo que a última situa o documento, sua principal fonte de estudo, como veículo do conhecimento codificado e formalizado por meio da linguagem. Desta forma, por meio da linguagem, ambas se contextualizam, uma quanto à gênese do conhecimento e a outra quanto à sua formalização.

Observa-se também que a percepção de si mesmo (auto-consciência) e do mundo é nitidamente um fenômeno informacional, ao mesmo tempo influenciando e sendo influenciado pelo contexto em que se insere o indivíduo. Esta concepção do conhecimento voltado à ação já fora

apontada, no contexto da Ciência da Informação, por Wersig (1993), entre outros. Ao formalizar seu pensamento, o indivíduo externaliza suas percepções e associa a elas uma conotação pragmática, voltada a influenciar os comportamentos dos receptores daquela comunicação. Os receptores, por sua vez, terão sua percepção do mundo modificada pelo conhecimento recém adquirido, percepção esta que dará origem a novas ações, num ciclo contínuo e renovado de geração e formalização do conhecimento. A efetividade destas interações será tanto maior quanto mais intensa forem a produção e a busca pelo conhecimento no contexto analisado, ou seja, quanto mais ativo for o comportamento informacional dos indivíduos considerados.

Desta forma, não causa estranheza que os comportamentos informacionais sejam outra área de proximidade entre a Fenomenologia e a Ciência da Informação, o que já fora apontado por, dentre outros, Wilson (1999) e Ng (2002), com especial destaque para a sociologia fenomenológica de Schutz, a qual encontra grande ressonância junto ao interacionismo simbólico de Blumer e que é influenciadora do *"sense making"* de Dervin (WILSON, 2002). Segundo a visão fenomenológica, o que se advoga aqui não é o uso das fontes de informação como mera redução de incertezas, mas sim a devida caracterização de problemas como sendo uma ruptura da concepção do mundo experimentada pelo observador: quando a percepção ou as atividades por ela encadeadas falham (por exemplo, quanto uma atividade de capacitação não surte o efeito desejado, para citar-se um exemplo do mundo organizacional), surge um "problema" do ponto de vista fenomenológico (MINGERS, 2001b). Em outras palavras, ocorre uma disparidade entre o objeto em observação e a sua imagem formulada pelo indivíduo.

Com vistas a sanar-se tal disparidade, os sistemas de informação, em vez de tentar impor um modelo estático e limitante, o que é uma prática usual, devem ser então projetados e construídos de modo aberto e flexível, respeitando as particularidades de cada domínio e provendo o compartilhamento de significados e de experiências - enfim, de conhecimento. Deste modo, humanizam-se os sistemas, além de expandir-se as fronteiras da organização, uma vez que por meio da comunicação realiza-se a troca de comportamentos (ações e percepções do mundo) entre os indivíduos, entre estes e as organizações e, por fim, entre as organizações vistas como sistemas (MERALI, 2002).

Um outro aspecto a salientar é o de que, além de importante ferramenta de análise de comportamentos, torna-se visível que a Fenomenologia pode cumprir o papel de suporte epistemológico, auxiliando a Ciência da Informação a situar-se perante outros domínios e a compreender melhor seus próprios objetos de estudo, bem como os métodos (CIBORRA, 1998) e as teorias que lhe dão embasamento (BATES, 1999), as disciplinas relacionadas (HJØRLAND, 2000) e

as interfaces adequadas entre usuários e sistemas (ZHANG; LI, 2004) [2].

Mas talvez a mais importante contribuição da Fenomenologia à Ciência da Informação, bem como a todas as outras ciências, seja a idéia de que não é possível ter-se uma percepção e uma observação "puras" do mundo. Sob esta concepção, similar à do realismo crítico, toda observação é dependente de uma teoria e de um contexto, estando continuamente sujeita a reformulações. As influências trazidas por esta visão de mundo estendem-se de Wittgenstein a Popper (MINGERS, 2004b, 2004a), com conseqüências fundamentais e permanentemente incidentes sobre o modo de produção científica ocidental.

3.4 Hermenêutica

Teóricos da fenomenologia como Ricoeur (1975) e Gadamer (1998) propuseram um relaxamento crítico dos severos requisitos apresentados por Husserl para a *epoché*, indicando que é impossível interpretar qualquer ação social sem que se reporte a algum conhecimento e experiência prévios. Para os mesmos autores, a linguagem, em todas as suas modalidades, é o modo fundamental de ser-no-mundo (WHITE, 1990). Este substrato lingüístico representa tanto o meio ou o instrumento pelo qual a comunicação se dá quanto, mais ainda, a abertura espaço-temporal compreendida como o ser-no-mundo (CAPURRO, 1982). É exatamente neste contexto que se apresenta a hermenêutica, comumente (e simplificadamente) conhecida como a ciência da interpretação de textos, mas que vem sendo continuamente rediscutida e atualizada (RISSER, 1997; VILLELA-PETIT, 2003; WILLIS, 2003) e que é cada vez mais utilizada em diferentes domínios (GEANELLOS, 2000; WIKLUND; LINDHOLM; LINDSTRÖM, 2002; LEONARDO, 2003; BEEBE, 2004), incluindo a ciência da informação (CAPURRO, 2000; HANSSON, 2005). A hermenêutica contrasta-se frontalmente com outras epistemologias, como o pragmatismo e o realismo (BAERT, 2003).

Uma das principais críticas ao paradigma normativo é a sua incapacidade de considerar eventos e elementos em processos ditos *whiteheadeanos* [3], ou seja, fenômenos que não se sucedem simplesmente, mas que se modificam de modo fundamental ao longo do tempo e de suas sucessivas interações. Deste modo, o paradigma normativo proporciona uma predição e uma explanação acuradas apenas para situações de interação particularmente rotineiras (DEETZ, 1973). O paradigma interpretativo, baseado na fenomenologia, na hermenêutica e na filosofia

[2] Tratando, por exemplo, como em Kim (2001), de uma fenomenologia do ser-digital.

[3] De Alfred North Whitehead, 1861-1947, matemático, logicista e filósofo britânico que, em companhia de Bertrand Russel, publicou os três volumes de *Principia Mathematica*, obra fundamental na lógica e metafísica do século XX.

da linguagem, por outro lado, busca substituir o senso comum por uma visão mais essencial que possa tornar públicos interpretações e significados que passem despercebidos no dia-a-dia (DEETZ, 1973) (HEIDEGGER, 1985, p. 188ss). Para tanto, três conceitos são fundamentais ao pesquisador (DEETZ, 1973):

implicação: considera-se o comportamento humano e seus produtos como a expressão de modos de ser-no-mundo. A ação humana, então, expressa-se ou implica em um modo de existência particular, ou seja, o conjunto de possibilidades de uso encontradas em um mundo humano - as escolhas implicativas somente se tornam explícitas quando consideradas na relação entre o comportamento específico e o modo de existência em que se apresentam;

interpretação: representa o elo entre o comportamento expresso e o modo de existência, entre a ação e suas escolhas, ou entre um comportamento e suas implicações; é uma "leitura" do mundo implicado a partir do ato concreto. A fim de visualizar a interpretação de um comportamento, não se deve olhar para o objeto que o gera, mas sim para as implicações (possibilidades de uso) que ele expressa.

linguagem: a interpretação, assim como no paradigma normativo, pressupõe uma linguagem *a priori*, já intersubjetivamente cheia de significados (segundo Dreyfus (1998), a linguagem tem o papel de chamar a atenção para algum aspecto do mundo já compartilhado) - a diferença consiste em que, enquanto o paradigma normativo considera a linguagem como sendo uma categoria residual que é simplesmente acrescentada ao comportamento uma vez disposto em uma classe definida (categorização), a abordagem interpretativa sugere que a natureza (as possibilidades implicadas) de um fenômeno comportamental seja idêntica ao comportamento conforme sua nomeação - o fenômeno é o seu nome, e observar um comportamento nomeado é observar seu mundo humano e as possibilidades implicadas.

A hermenêutica busca, desde modo, identificar um comportamento que expressa um mundo percebido e o entendimento do mundo que interpreta e explica o comportamento (DEETZ, 1973, p. 150), em uma co-determinação que baseia o assim chamado "círculo hermenêutico" - um movimento de ir e vir entre idéias pré-concebidas (pré-conceitos) que são trazidas ao debate e os *insights* daí advindos (PIERCEY, 2004). Uma visão esquemática desta rede de atuação está ilustrada na Figura 3.

Nota-se que a ação hermenêutica se dá com base na observação de comportamentos manifestos, escritos ou salientes, o que Ricoeur chama de "ação como texto" (RICOEUR, 1991,
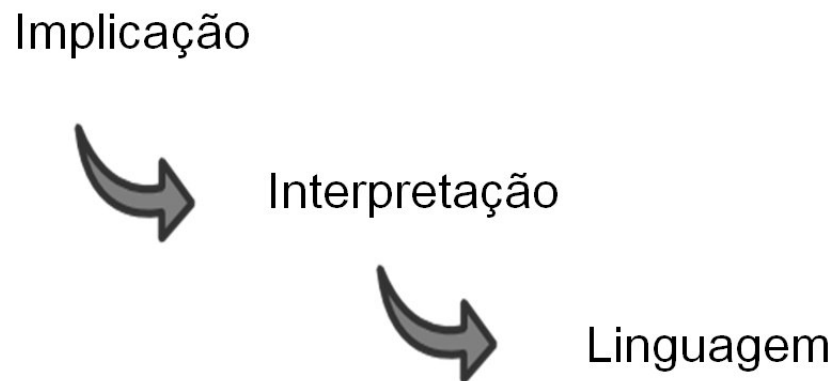
Figura 3: Rede de atuação observada no paradigma interpretativo.

p. 82). Ainda acerca desse mesmo tema, para Ricoeur (1990, p. 33), o papel da hermenêutica consiste na compreensão destes textos, mas "compreender um texto não é descobrir um sentido inerte que nele estaria contido, mas revelar a possibilidade de *ser* indicada pelo texto". O mesmo autor conceitua ainda a hermenêutica como sendo a "teoria das operações de entendimento em sua relação com a interpretação de textos" (RICOEUR, 1982, p. 43) e segue afirmando que "o objetivo da interpretação é produzir um discurso relativamente unívoco a partir de palavras polissêmicas e identificar esta intenção de univocidade na recepção das mensagens" (RICOEUR, 1982, p. 44). Mais adiante, Ricoeur salienta ainda que a fenomenologia permanece como a insuperável pressuposição da hermenêutica, ao mesmo tempo que a fenomenologia não pode se constituir sem uma pressuposição hermenêutica (RICOEUR, 1982, p. 101). Deste modo, fenomenologia e hermenêutica estão intrinsecamente associadas.

Questões acerca da corretude, plausibilidade ou verificação do entendimento embutido no paradigma interpretativo, segundo Deetz (1973, p. 152), são irrelevantes, uma vez que a postura histórica do pesquisador é uma constituinte da natureza e das implicações do comportamento observado - o comportamento como descrito não pode ser visto sem a interpretação que lhe foi dada. A fim de garantir-lhe objetividade e validade, alguns critérios metodológicos devem ser observados (DEETZ, 1973, p. 153ss):

- por princípio, o comportamento humano ou os seus produtos devem ser vistos como ações simbólicas, cuja natureza é composta pelas possibilidades implicadas e inseridas em um mundo sugerido por tais possibilidades;
- os fenômenos humanos devem ser compreendidos na linguagem do mundo experiencial do qual fazem parte;
- alguns critérios devem ser alcançados, tais como:
  - legitimidade: a interpretação atribuída é uma possibilidade na linguagem da comunidade?
  - correspondência: todos os comportamentos observados expressam o mesmo mundo implicativo?
  - apropriação de gênero: diferentes tipos de comportamento devem ser adequadamente interpretados de diferentes formas;
  - coerência: as implicações expressas são inteligíveis e plausíveis?
- o ponto de vista do indivíduo não deve ser literalmente considerado nem deve ser usado como critério para avaliar a interpretação - o comportamento objetivo expressa mais adequadamente o mundo de possibilidades implicadas;
- a intuição, quando vista como conhecimento essencial metodologicamente embasado, deve ser diferenciada da introspecção inferencial e do subjetivismo impressionista;
- não se exige que o pesquisador se envolva diretamente no mundo sob escrutínio, mas que a interpretação-entendimento-explicação seja expressa na linguagem do mundo do comportamento observado a fim de se adequar e expressar de modo autêntico a estrutura de possibilidades implicativas.

No que diz respeito à segurança da informação, são usuais as interpretações segundo as quais um sistema de informações é composto pelo complexo de tecnologia (hardware e software), enquanto outras dão um pequeno passo adiante ao abarcar a presença do usuário. Contudo, conforme já se disse, o usuário não é um indivíduo isolado - ele vive em determinado contexto (organizacional, no interesse deste trabalho) e com ele interage, ao mesmo tempo influenciando-o e por ele sendo influenciado. Assim sendo, apresenta-se a seguinte definição:

Definição 3.1 *O **usuário** de um sistema de informação é o indivíduo diante do qual se concretiza o fenômeno do conhecimento provido por aquele sistema.*

Com base nestes requisitos e adotando-se a postura descrita neste capítulo, passa-se ao estudo propriamente dito do contexto da segurança da informação.

4 O contexto da segurança da informação

4.1 Conceitos básicos

A FIM de melhor compreender-se a inserção da segurança da informação sob os diferentes aspectos em que se apresenta, tendo em vista evitar-se o reducionismo tecnológico sob o qual é geralmente apresentada, é fundamental que ela seja vislumbrada à luz de alguns dos conceitos da disciplina da qual é tributária - a Ciência da Informação. Ambas focalizam a informação do ponto de vista de seus aspectos estruturais, reconhecendo que conceitos como "significado", "valor" e "relevância", quaisquer que sejam seus entendimentos, são dependentes do contexto organizacional em que se insere o objeto de seu estudo ou aplicação, qual seja, a informação em si mesma. Deste modo, a interação entre a segurança e o contexto organizacional, interação esta que se manifesta sob as nuances da cultura organizacional e do comportamento individual perante o ambiente informacional, deve ser igualmente foco de interesse da segurança, como se verá em detalhes adiante. De antemão, cumpre salientar-se a seguinte evidência: o grau de "valor" e de "relevância" conferido à segurança da informação pela organização deve estar diretamente relacionado ao grau dos mesmos conceitos quanto aplicados à informação.

Outro conceito extremamente valioso à Ciência e à segurança da informação é o da interdisciplinaridade. O caráter interdisciplinar, no tocante à Ciência da Informação, é direta ou indiretamente abordado por vários estudiosos do tema e permeia um sem-número de discussões e relatos históricos, tais como as asserções e considerações apresentadas por Saracevic (1995, 1999) e Lesk (1995). Contudo, quer-se enfatizar aqui o que já fora enunciado por Bates (1999), ao apontar a Ciência da Informação como elemento central às atividades de representação e organização da informação. Em seu texto, a autora aponta que o domínio da Ciência da Informação é o universo da informação registrada, selecionada e armazenada para acesso posterior, salientando ainda que a representação da informação difere do seu conhecimento;

no presente trabalho, ressalta-se que, na mesma extensão em que não se pode imaginar o conhecimento sem a representação da informação, a segurança difere dos meios de coleta, armazenamento e disseminação, mas não pode prescindir deles para sua subsistência. Mais ainda, num arco simétrico, é exatamente a segurança que visa proporcionar a estes meios a garantia de atingirem adequadamente os seus objetivos. A fim de elucidar este paralelo que se deseja criar e para caracterizar-se adequadamente a segurança da informação tal como se procura entendê-la em suas diversas nuances, cabe introduzir-se alguns dos elementos básicos concernentes ao tema, apresentando sua abrangência e complexidade.

4.1.1 A Informação e seu ciclo de vida

O conceito de informação tem sido discutido e apresentado sob diferentes facetas por diferentes autores, a depender do contexto em que se realiza a explanação. Desnecessário dizer que cada faceta é complementar às demais. Apenas para citar-se alguns exemplos, Shannon (1948) apresenta-a como um elemento mensurável e dependente do âmbito de seu emissor e receptor, ao passo que Henessy e Babcock (1998), por sua vez, situam a informação como indicadora de variabilidade controlada. De um modo geral, aceita-se que aliado ao fenômeno da informação situa-se o da comunicação, quer de modo implícito, como em Braga (1995), quer de modo explícito, como em Saracevic (1999), sendo que neste último autor os aspectos de transferência e compartilhamento são salientados.

Anteriormente reconhecida por seu papel como redutora de incertezas, a informação é cada vez mais vista como um recurso transformador do indivíduo e da sociedade, cabendo-lhe papel essencial no contexto sócio-econômico vigente, não por acaso denominado de "Era da Informação". As características da informação que são atualmente mais salientadas são as seguintes:

Valor: valoriza-se não somente o que se sabe, mas também, e em muitos casos até mais, o que não se sabe. Transações entre indivíduos, empresas e governos são cada vez mais baseadas na troca de informações, que substituem os ativos tangíveis e o papel-moeda. O grau de conhecimento a respeito dos bens de troca e da situação dos prováveis parceiros ou concorrentes, por sua vez, assume papel cada vez mais preponderante. Diversos modelos para a valoração da informação têm sido apresentados, tais como o de Dickhaut et al. (2003) e o de Henessy e Babcock (1998). Em comum, apresentam a preocupação com a distribuição da informação entre os participantes, quer em situações de parceria, como consorciados, quer em situações de rivalidade, como concorrentes.

Temporalidade ou volatilidade: tão importante quando "o que" se sabe é "quando" se sabe.

O exemplo das informações noticiosas é apenas um dentre a gama que se pode citar: o que hoje é um "furo" amanhã tornar-se-á uma notícia velha. Quando a este critério, varia-se da situação em que a informação deve estar disponível no instante exato em que dela se necessite (caso de permissão de acesso concedida) à situação em que ela não deve estar disponível em tempo algum (caso de permissão de acesso vedada). Observe-se que a temporalidade está, em muitos casos, instrinsecamente relacionada ao valor e ao usuário em questão.

Abrangência: mede o número de usuários (sejam eles humanos ou sistemas automatizados) com o qual a informação se relaciona, bem como o nível hierárquico em que se encontram. Em muitos casos, quanto maior o valor da informação tratada, menor sua abrangência, mas há pelo menos um caso em que isto não se verifica: a chamada lei de Metcalfe, segundo a qual o valor de um sistema de comunicação é proporcional ao quadrado do número de seus usuários (ANDERSON, 2001) - observe-se que a informação é parte integrante do sistema de comunicação, como na internet, para citar-se o exemplo mais evidente.

Extensibilidade: mede o grau com que a informação é capaz de originar mais informação, de valor e relevância comparáveis ou superiores à informação original. Apenas para citar-se um exemplo, este é um dos pilares da comunidade de software aberto, mas deve-se ressaltar que isto não implica a gratuidade da informação assim disseminada. A gestão do conhecimento, com seu enfoque voltado à formação e à preservação do capital intelectual, é outra área afeita a este conceito.

O texto clássico de Borko (1968), ao situar o escopo da Ciência da Informação, aponta para as principais etapas do ciclo de vida da informação: origem, coleta, organização, armazenagem, recuperação, interpretação, transmissão, transformação e utilização. Todas estas etapas estão sujeitas a eventos afeitos à segurança, sendo que estes eventos podem ocorrer em momentos precoces ou tardios de cada uma das etapas, o que faz com que a segurança da informação tenha de se preocupar com todo o ciclo de vida, sem desprezar nenhuma das etapas identificadas.

O fato de que, cada vez mais, os recursos de tratamento da informação (ou seja, os recursos que manipulam a informação durante o seu ciclo de vida) sejam apresentados sobre uma base tecnológica induz a que se dê elevada ênfase aos aspectos tecnológicos da segurança. De fato, esta ênfase não é recente (SALTZER; SCHROEDER, 1975). Entretanto, não deve ser a tecnologia a única nuance contemplada - nem mesmo a principal. A elevada presença tecnológica pode ser ilustrada pela Figura 4, obtida do projeto Metrometá da Universidade de Montreal (TURNER; MOAL, 2003), que mostra algumas das etapas do ciclo de vida e a utilização da

tecnologia em unidades de informação. Nesta acepção, todos as etapas do ciclo representadas estão fortemente calcadas em protocolos e ferramentas tecnológicas.
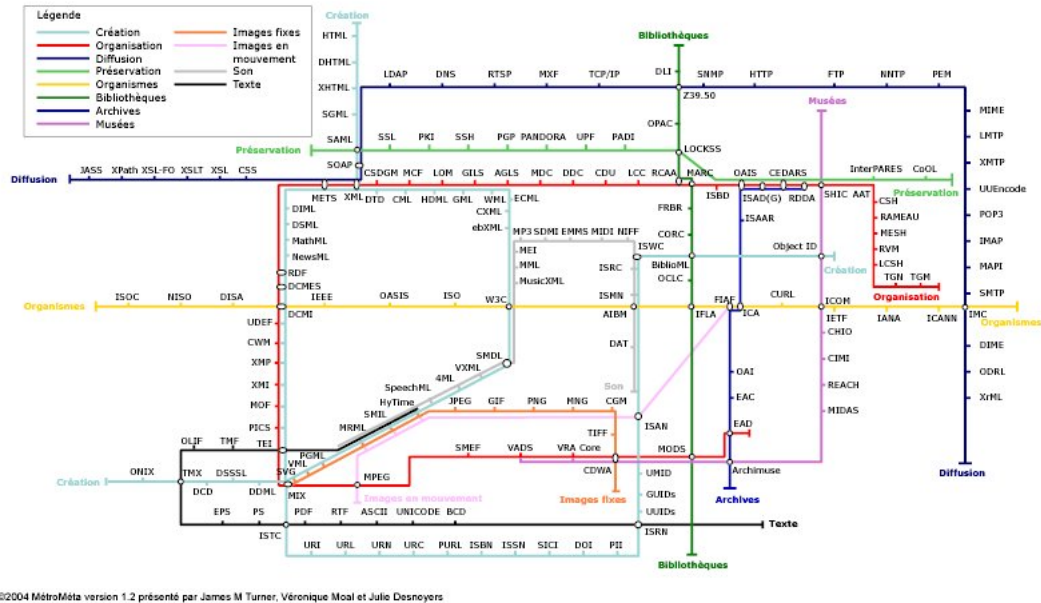
Figura 4: Etapas do ciclo de vida e algumas unidades de informação. Fonte: Turner e Moal (2003).

A fim de que se possa situar adequadamente o escopo da segurança da informação, alguns conceitos devem sem introduzidos.

4.1.2 Ativos da informação

É usual a visão de que a informação constitui *per se* um ativo (no sentido de ser um bem a ser valorizado e preservado) (SÊMOLA, 2003, pp. 1-2). Contudo, na visão deste trabalho, a concepção de ativo da informação (ou ativo informacional, como também é comum chamar-se) compreende o conjunto dos indivíduos, compostos tecnológicos e processos envolvidos em alguma das etapas do ciclo de vida da informação. Embora seja uma relação óbvia, deve-se enfatizar que a relevância desta participação é determinante para a estabelecimento dos aspectos da segurança envolvidos: é comum dar-se especial atenção a ativos específicos, como os mais caros ou os menos comuns; mas quanto mais intensa for a participação do ativo no ciclo de vida, tanto maior a prioridade com a qual aquele ativo deve ser considerado no tocante à segurança da informação de cujo ciclo participa. Percebe-se, então, que mesmo os ativos considerados desprezíveis, por serem de baixo custo ou abundantes, por exemplo, podem gerar impacto decisivo

sobre a segurança da informação à qual estão relacionados [1]. Deste modo pessoas, sistemas, equipamentos e os próprios fluxos seguidos pelos conteúdos informacionais devem ser devidamente considerados por ocasião da planificação da segurança da informação. Perceba-se que, uma vez que a informação seja qualificada como sensível, realiza-se uma abstração quanto a conceitos como o seu conteúdo, volume ou mesmo formato, exceto para fins de implementação de mecanismos físicos de preservação (que diferem entre mídias digitais e impressas, por exemplo), adotando-se os mesmos procedimentos para diferentes conteúdos e acervos.

Estando dispersos nos ambientes organizacionais, os ativos da informação estão sujeitos a diversos eventos e potencialidades nocivos à sua segurança, divididos em três categorias: ameaças, vulnerabilidades e incidentes, os quais compõem e caracterizam os riscos.

4.1.3 Ameaças

Uma das definições apresentadas para ameaça é "evento ou atitude indesejável (roubo, incêndio, vírus, etc.) que potencialmente remove, desabilita, danifica ou destrói um recurso" (DIAS, 2000, p. 55). A mesma autora apresenta o item recurso como sendo "componente de um sistema computacional, podendo ser recurso físico, software, hardware ou informação" (DIAS, 2000, p. 55). Perceba-se que não se fala sobre o recurso humano - a esta altura, o leitor deste trabalho já se deve ter percebido como este componente tem importância fundamental sobre todos os eventos afeitos à segurança da informação. Esta vertente acredita, assim, que o homem pode ocasionar algum dano ao sistema, mas não se reconhece que ele pode ser também uma vítima de algum ato, deliberado ou não, capaz de ocasionar a ele ou à organização uma perda informacional sensível. Acrescente-se a isto o fato de que, embora muitos gestores aleguem reconhecer a segurança da informação como importante, nem sempre lhe é dada a sua real relevância, e tem-se um quadro não muito animador sobre o tema.

Com o advento das redes de longo alcance, principalmente a internet, tem-se uma característica complicadora para este cenário: a capacidade de anonimato, ou mesmo de *desindividualização* (ausência de características que permitam a identificação de autoria) das ações executadas em rede. Um usuário pode, em tese, se fazer passar por virtualmente qualquer outra pessoa, não importando de que etnia, gênero ou grupo social, desde que esteja disposto a tanto e tenha acesso aos recursos computacionais requeridos para esta tarefa, os quais são, em geral, exíguos. Tal situação é a tal ponto crítica que leva, em muitos casos, à adoção obrigatória de mecanismos de identidade eletrônica, como a certificação digital, à procura de modalidades

[1]Pode-se comparar esta situação à súbita falta de um insumo comum na linha de produção de um determinado bem, como a ausência de carvão numa usina siderúrgica.

seguras de autenticação de usuários. A este respeito, a charge ilustrada pela Figura 5 é particularmente esclarecedora. Cumpre observar, ainda, que um usuário pode se surpreender ao realizar uma pesquisa em um dos vários sítios de busca na web, sejam os de pesquisa textual como o *Google* [2], o *Altavista* [3] ou o *Yahoo* [4], sejam os de pesquisa contextualizada como o *Kartoo* [5] ou o *Mooter* [6], usando como argumento de pesquisa o seu próprio nome ou os nomes de pessoas conhecidas.

Figura 5: *Desindividualização* na *web*. Fonte: Steiner (1993).

Como exemplo de análise de ameaças à segurança da informação em ambientes computacionais, cite-se o estudo realizado em 2002 por Whitman (2003), o qual procurou responder a três questões primordiais:

1. quais são as ameaças à segurança da informação?
2. quais são as mais danosas ao ambiente organizacional?
3. qual a freqüência com que eventos baseados nelas são observados?

[2]www.google.com
[3]www.altavista.com
[4]www.yahoo.com
[5]www.kartoo.com
[6]www.mooter.com

Em resposta à primeira pergunta, foram listadas doze categorias de ameaças potenciais, obtidas a partir de trabalhos anteriores e da entrevista com três *security officers*. Estas doze categorias são as seguintes, já dispostas em ordem decrescente de severidade percebida, conforme respostas obtidas pelo *survey* online realizado com organizações de diferentes portes e áreas de atuação (o autor não cita o número de instituições envolvidas na pesquisa):

1. eventos deliberados cometidos com o uso de software (vírus, vermes, macros, negações de serviço);
2. erros ou falhas técnicas de software (falhas de codificação, *bugs*);
3. falhas ou erros humanos (acidentes, enganos dos empregados);
4. atos deliberados de espionagem ou invasão, *hacking*;
5. atos deliberados de sabotagem ou vandalismo (destruição de sistemas ou informação);
6. erros ou falhas técnicas de hardware (falhas de equipamentos);
7. atos deliberados de furto (de equipamentos ou de informação);
8. forças da natureza (terremotos, enchentes, relâmpagos, incêndios não intencionais);
9. comprometimento à propriedade intelectual (pirataria, infração a direitos autorais);
10. variação da qualidade de serviço (*Quality of Service* - *QoS*) por provedores (como energia elétrica e serviços de redes remotas de telecomunicação);
11. obsolescência técnica; e
12. atos deliberados de extorsão de informação (chantagem ou revelação indevida de informação).

Quanto à freqüência, os dados coletados por Whitman (2003) apontaram os resultados listados na Tabela 3.

4.1.4 Vulnerabilidades

Uma vulnerabilidade representa um ponto potencial de falha, ou seja, um elemento relacionado à informação que é passível de ser explorado por alguma ameaça - pode ser um servidor ou sistema computacional, uma instalação física ou, ainda, um usuário ou um gestor de informações consideradas sensíveis. Dada a incerteza associada aos ativos e às vulnerabilidades

Número de eventos por mês	Nenhum	Até 50	De 51 a 100	Mais de 100	Sem Resposta
1. Eventos por software	16,7	62,5	9,4	11,5	
2. Erros ou falhas técnicas de software	30,2	64,6	5,2		
3. Falhas ou erros humanos	24,0	66,3	2,1	5,2	12,5
4. Espionagem ou invasão (*hacking*)	68,8	23,9	3,1	4,2	
5. Sabotagem ou vandalismo	64,6	34,4		1,0	
6. Erros ou falhas técnicas de hardware	34,4	62,5	3,1		
7. Furto	54,2	45,8			
8. Forças da natureza	62,5	36,5		1,0	
9. Comprometimento à propriedade intelectual	61,5	28,1	2,1	1,0	7,3
10. Variação de QoS	46,9	52,1	1,0		
11. Obsolescência técnica	60,4	37,5	1,0		1,0
12. Extorsão	90,6	9,3			

Tabela 3: Número mensal de eventos por ameaça, em percentual de respondentes (adaptada de Whitman (2003)).

a eles relacionadas, a construção de modelos probabilísticos tem sido utilizada para o mapeamento dos diferentes elementos da informação, na construção dos conjuntos de vulnerabilidades associadas a cada ativo. As diferentes soluções tecnológicas utilizadas na redução de vulnerabilidades sofrem de uma falha extremamente severa: estão em geral orientadas a vulnerabilidades específicas e sua utilização, potencialmente, pode introduzir novas vulnerabilidades. Diversas soluções têm sido tentadas, como a aplicação de algoritmos genéticos para a criação de perfis de segurança voltados a situações genéricas (GUPTA et al., 2004), mas um longo caminho ainda está por ser percorrido. Também o prognóstico de vulnerabilidades, ou seja, a tentativa de identificar áreas ou servidores computacionais em uma rede que podem se mostrar vulneráveis em um momento futuro, com o uso de recursos como lógica nebulosa (VENTER; ELOFF, 2004), carece de maiores desenvolvimentos.

Há que se observar que estas e outras propostas, dependentes de recursos tecnológicos como são, podem se ver, por si mesmas, sujeitas a vulnerabilidades, realimentando o ciclo de procura por soluções efetivas ao problema. De fato, o relatório IT Governance Institute (2004c) indica que grande parte dos gestores enxergam a importância da Tecnologia da Informação - TI para atingir a estratégia da organização, mas 41% dos respondentes a este *survey* vêem como problema uma visão inacurada da performance da tecnologia da informação - ou seja, não têm um panorama claro do andamento do setor de informação em suas próprias organizações.

4.1.5 Incidentes

O *Internet Engineering Task Force* - IETF, organização independente dedicada à análise e prevenção de eventos de segurança e à gestão da rede, define incidente como sendo "um evento que envolve uma violação de segurança" (SHIREY, 2000). Uma definição mais voltada à autoria e ao tipo do evento é dada por Howard e Meunier (2002): "um ataque ou um grupo de ataques que pode ser diferenciado de outros ataques pela distinção dos atacantes, ataques,

objetivos, *sites* e ocasião".

4.1.6 Ataques

Por sua vez, um ataque corresponde à concretização de uma ameaça, não necessariamente bem-sucedida (do ponto de vista do atacante), mediante uma ação deliberada e por vezes meticulosamente planejada.

Uma vez que a geração de ataques é originada por pessoas, ainda que com o uso de recursos computacionais ou de outra natureza, a sua prevenção torna-se extremamente complexa por meios automatizados. De fato, Schell (2001) afirma que não há ciência capaz de eliminar definitivamente os incidentes de segurança da informação, restando a opção da constante vigilância e verificação.

Deve-se observar, ainda, que os ataques podem ser de origem externa ou interna à organização. Schultz (2002) aponta que os ataques de origem interna, que, ao contrário do que se apregoa, não necessariamente são em maior número que os externos, possuem motivações e padrões diversos daqueles, exigindo, assim, análise e contramedidas diferenciadas.

4.1.7 Riscos

Diversas abordagens têm sido apresentadas para o tratamento de riscos, ou para averiguar de que maneira a prevenção de riscos pode influenciar a gestão da segurança da informação. De qualquer modo, é consensual que o risco deve ser adequadamente medido e avaliado, possibilitando a criação de medidas preventivas voltadas à sua diminuição.

O risco pode ser definido como as perdas, incluindo perdas em vidas humanas, que podem ocorrer mediante a adoção de determinado curso de ação. Pode-se medir o risco em termos da utilidade monetária envolvida ou pela variância da distribuição de probabilidade de eventuais perdas e ganhos associados a alguma alternativa em particular. É senso comum que o risco jamais pode ser integralmente eliminado (GUAN et al., 2003). Ao se engajar em atividades de avaliação e prevenção de riscos, as organizações têm em vista este senso comum.

A norma BS7799, formulada pelo British Standards Institute e que inspirou a norma ISO/IEC 17799, cuja primeira parte [7] foi implementada no Brasil por meio da norma NBR 17799, descreve os controles de segurança requeridos no ambiente organizacional e preconiza que os sistemas de gestão de segurança da informação devem se focam na gestão de riscos a fim de atingir

[7] A segunda parte diz respeito à implementação de modelos de sistemas de gestão de segurança da informação e foi recentemente publicada sob o número 27001:2005.

os seguintes objetivos (GUAN et al., 2003):

- identificar o valor e analisar eventuais fraquezas dos ativos de informação;
- permitir que a gerência tome decisões fundamentadas sobre a gestão do risco, eventualmente justificando despesas alocadas a este fim; e
- incrementar a informação organizacional sobre os sistemas de tecnologia da informação a fim de melhorar sua segurança.

A avaliação de riscos compreende nove passos, a saber (GUAN et al., 2003):

1. caracterização do sistema;
2. identificação de ameaças;
3. identificação de vulnerabilidades;
4. análise dos controles utilizados;
5. determinação da probabilidade dos eventos listados nos passos anteriores;
6. análise de impacto;
7. determinação dos riscos;
8. recomendação de controles a utilizar; e
9. documentação dos resultados.

Guan et al. (2003) ressaltam ainda que, caso haja registros históricos consistentes e dados estatísticos plausíveis, pode-se utilizar uma das seguintes fórmulas para a determinação do valor do risco (custo das perdas):

$$R = W \times X \times V \tag{4.1}$$

$$R = \frac{V(10^{C+W-3})}{3} \tag{4.2}$$

onde R é o valor do risco, W é a probabilidade ou verossimilhança da ocorrência de ataques, C é o custo total do ativo e V é a vulnerabilidade a que está sujeito o ativo. Na ausência de dados

históricos, é usual que se estime os valores de W e V com base em dados externos, tais como seguradoras ou organizações de mesmo porte ou segmento.

A ausência de acurácia observada na obtenção destes dados e a complexidade envolvida na gestão da segurança dos ativos de informação levam à apresentação de um sem-número de propostas de modelos para o seu tratamento. Estes modelos variam desde a identificação *in loco* de ativos, ameaças e vulnerabilidades (FARN; LIN; FUNG, 2004), passando pela mensuração do risco com o uso de métodos quantitativos baseados em *surveys* direcionados a organizações (KARABACAK; SOGUKPINAR, 2005), indo até a definição de metodologias completas de mensuração e tratamento de riscos (ALBERTS; DOROFEE, 2002), sua análise sob um enfoque transdisciplinar (HORLICK-JONES; SIME, 2004) e a proposta de regulamentação da análise e tratamento de riscos à informação em setores específicos, como a informação médica (ALBERTS; DOROFEE, 2004).

Todas estas iniciativas, contudo, esbarram em um problema essencial: seria a percepção do risco a mesma entre os especialistas em segurança, entre os gestores da informação e entre os usuários da informação em tais contextos informacionais? Stewart (2004) alerta para esta questão, enquanto Jasanoff (1998) suscita um problema correlato: seria o risco *percebido* de fato compatível com o risco *real*?

Além disso, o próprio uso da tecnologia de controle de riscos impõe o surgimento de novos riscos, antes ausentes, alimentando um ciclo aparentemente infindável (CIBORRA, 2004).

A resposta a estas perguntas passa pela compreensão de que diferentes indivíduos têm diferentes percepções a respeito de um mesmo assunto, uma asserção tão evidente quanto negligenciada no contexto da segurança da informação. A segurança da informação carece, assim, de meios que dêem suporte à coleta e à avaliação corretas da percepção dos usuários quanto aos elementos (ativos, ameaças, vulnerabilidades, incidentes e riscos) da segurança relativos aos sistemas com os quais interagem.

4.2 O conceito vigente de Segurança da Informação

A literatura especializada é pródiga na apresentação de conceitos do que a segurança da informação *faz* e de quais são os domínios de sua atuação, mas não do que ela de fato *é*. Ou seja, abundam as análises funcionais, mas são escassas as análises descritivas da segurança da informação.

Pemble (2004) sugere que a segurança da informação deve ser definida em termos das

atribuições do profissional que é responsável por ela. O artigo descreve três esferas de atuação de tais profissionais, em torno das quais a segurança deveria ser parametrizada e compreendida:

- a esfera operacional, voltada ao impacto que os incidentes podem gerar à capacidade da organização de sustentar os processos do negócio;
- a esfera da reputação, voltada ao impacto que os incidentes têm sobre o valor da "marca" ou sobre o valor acionário; e
- a esfera financeira, voltada aos custos em que se incorre na eventualidade de algum incidente.

Arce (2003a) lembra que diversos tipos de ataques em redes produzem resultados sobre a informação no nível semântico, ou seja, atuam sobre o significado da informação, modificando-o. A mudança de rotas de acesso em redes e a falsificação de endereços de servidores computacionais são exemplos destes ataques. Contudo, as ferramentas de detecção e prevenção atuam no nível sintático: elas tratam cadeias de caracteres em busca de padrões ou seqüências não esperadas, como é o caso de um software anti-vírus ou de uma ferramenta de prevenção de intrusões. Esta diferenciação produz um descompasso evidente entre "caça" (atacante) e "caçador" (profissional da segurança): eles simplesmente atuam em níveis epistemológicos distintos, requerendo abordagens diferenciadas das atualmente utilizadas para a solução efetiva do problema.

Uma das frases mais citadas no contexto da segurança da informação é que "uma corrente é tão resistente quanto seu elo mais fraco". É comum a asserção de que o elo mais fraco da corrente da segurança da informação seja o usuário, uma vez que os recursos computacionais já estariam protegidos por considerável acervo tecnológico... Arce (2003b) sugere que os sistemas operacionais das estações de trabalho e seus usuários seriam os mais vulneráveis a ataques internos e externos - contudo, como já se viu, o complexo que a segurança abrange requer atenção a todos os níveis de usuários e sistemas.

Outro aspecto que se tem mostrado extremamente relevante é o custo da segurança da informação. Geer Jr, Hoo e Jaquith (2003) mostram o custo relativo para a correção de falhas de segurança em softwares em cada estágio do processo de desenvolvimento, conforme ilustra a Tabela 4. Como se vê, quanto mais tardiamente as falhas são detectadas e corrigidas, tanto maior é o custo em que se incorre.

Ainda, Venter e Eloff (2003) sugerem uma taxonomia para as tecnologias de segurança da informação, dividindo-as em reativas e proativas, baseando-se no clássico modelo de redes em

Estágio	Custo relativo
Projeto	1,0
Implementação	6,5
Testes	15,0
Manutenção	100,0

Tabela 4: Custo relativo da segurança no desenvolvimento de software. Fonte: Geer Jr, Hoo e Jaquith (2003).

sete camadas da *Open Systems Interconnection* - OSI.

Todas as definições e proposições acima baseiam-se ou derivam de conceitos da segurança da informação sendo vista como um domínio tecnológico, onde ferramentas e recursos tecnológicos são aplicados em busca de soluções de problemas gerados, muitas vezes, com o concurso daquela mesma tecnologia. Evidencia-se a necessidade de uma compreensão mais abrangente destes problemas.

4.2.1 A necessidade de um novo conceito de segurança da informação

A ausência de um conceito exato do que seja a segurança da informação já foi abordada, entre outros, por Anderson (2003). O autor cita vários textos que sugerem uma definição para o termo, mas que na verdade apresentam as atribuições ou resultados esperados pela aplicação da segurança da informação. Ele apresenta seu próprio conceito: "Um sentimento bem fundamentado da garantia de que os controles e riscos da informação estão bem equilibrados", discorrendo em seguida sobre cada uma das partes componentes da definição, à qual voltar-se-á em breve.

Hitchings (1995) apresentava, já há mais de uma década, a necessidade de um conceito de segurança da informação no qual o aspecto do agente humano tivesse a devida relevância, tanto como agente como paciente de eventos de segurança (ataques, mais especificamente).

Mesmo no aspecto tecnológico, sugestões como a de Stergiou, Leeson e Green (2004) de um alternativa ao modelo da OSI, ou como a de Aljareh e Rossiter (2002) de um modelo de segurança colaborativo, têm sido apresentadas em contraposição ao modelo vigente.

4.3 Incidentes de segurança da informação

A literatura, principalmente a não especializada, é rica em relatos de incidentes de segurança da informação. Na verdade, para o público leigo, este é o aspecto mais saliente da segurança: ela é muito mais conhecida por suas falhas e imperfeições que pelos sucessos que possa

vir a colher.

Furnell, Chiliarchaki e Dowland (2001) apresentam um problema particularmente sensível para os profissionais de segurança da informação: o uso de ferramentas de segurança para perpetrar ataques. Com a disseminação de soluções de código aberto, muitas ferramentas originalmente desenvolvidas para a detecção de vulnerabilidades em redes, por exemplo, são distribuídas gratuitamente em praticamente todo o mundo. Este argumento, por sinal, tem sido utilizado por opositores ao modelo de software de código aberto, mas com conseqüências presumivelmente limitadas.

4.3.1 Incidentes de segurança da informação no contexto global

Uma dos mais completos levantamentos voltados à segurança da informação nos E.U.A é a pesquisa anual realizada em conjunto pelo *Computer Security Institute* - CSI e pelo *Federal Bureau of Investigations* - FBI. A edição de 2004, a nona realizada e cujos resultados foram divulgados em julho daquele ano, foi feita junto a 494 profissionais de segurança da informação que atuam em corporações e agências governamentais, instituições financeiras e médicas e universidades. Alguns dos resultados apontados foram os seguintes (GORDON et al., 2004):

1. o uso não autorizado de sistemas computacionais está em declínio, ao menos no que diz respeito às perdas financeiras ocasionadas por este tipo de ataque;

2. o tipo de ataque que se tornou o mais dispendioso passou a ser a negação de serviço ou DoS (*Denial of Service*), por meio do qual o atacante direciona a um ou mais servidores computacionais um volume de solicitações muito superior à sua capacidade de atendimento, terminando por incapacitá-lo; este ataque pode ser originado de uma única fonte ou de vários outros computadores controlados pelo atacante, na modalidade conhecida como negação de serviço distribuída ou DDoS (*Distributed Denial of Service*);

3. o percentual de organizações que informa aos agentes da lei a ocorrência de intrusões por computador tem diminuído, devido à preocupação com publicidade negativa;

4. a maioria das organizações enxerga o treinamento voltado a práticas de segurança da informação como importante, mas respondentes de todos os setores informaram não acreditar que sua organização invista o suficiente nesta área.

O percentual do orçamento de TI gasto em segurança pelas instituições pesquisadas, no período de coleta dos dados, é ilustrado pela Figura 6. Observe-se a alta concentração em fatias

de percentual igual ou inferior a 5%.
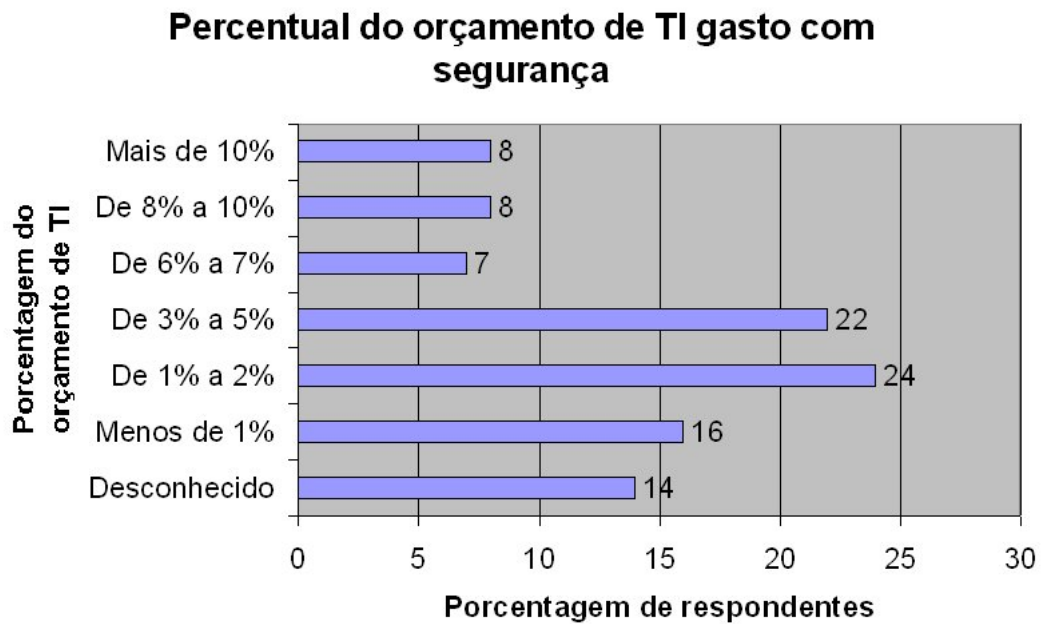
Figura 6: Percentual do orçamento de tecnologia da informação gasto em segurança (2003-2004). Fonte: Gordon et al. (2004).

Conforme já se salientou, a lista de incidentes envolvendo computadores não se resume a ataques deliberados. Falhas em sistemas computacionais, seja em componentes de software, seja em componentes de hardware, têm provocado desde *blackouts* de grandes proporções a falhas em robôs utilizados nos programas de exploração espacial (NEUMANN, 2004). Com efeito, no tocante ao software, tem-se observado um aumento significativo no número de falhas por aplicação (GEER JR; HOO; JAQUITH, 2003). Este fato também aponta para a necessidade da formulação adequada dos requisitos da segurança de informação no projeto de software, não fossem suficientes os valores relativos listados na Tabela 4.

Outro aspecto de vital importância num contexto econômico global e em ebulição diz respeito ao tratamento da informação quando ocorre a fusão ou incorporação de uma instituição por outra (WILSON, 2004). Os usuários dos sistemas devem ser afetados de modo a gerar impacto mínimo, enquanto as informações e transações assumem conformidade compatível com a nova realidade econômica.

Ainda no mundo corporativo, o relatório da consultoria Ernst & Young, realizado junto a mais de 1.600 organizações de 66 países e apresentado em 2003, indica os seguintes resultados auspiciosos (E&Y, 2003):

1. 90% das organizações respondentes indicam que a segurança da informação é de alta importância que atinjam seus objetivos;

2. 78% das organizações indicam a redução do risco como a maior influência decisória sobre onde investir em segurança da informação.

Porém, o mesmo *survey* aponta as seguintes conclusões (E&Y, 2003):

1. mais de 34% das organizações se reconhecem incapazes de determinar se seus sistemas de informação estão sob ataque;
2. mais de 33% das organizações reconhecem ter capacidade inadequada para responder a incidentes de segurança da informação;
3. 56% das organizações alegam ter em um orçamento insuficiente o principal obstáculo a uma postura eficiente no tocante à segurança da informação;
4. apenas 35% das organizações alegam possuir programas permanentes de educação e alerta quanto à segurança da informação.

O panorama se mostra ainda mais crítico quando se observa que algumas das soluções tecnológicas mais utilizadas no âmbito da segurança, como os sistemas criptográficos, apresentam em alguns casos falhas graves de implementação (ANDERSON, 1993; SCHNEIER, 2000), comprometendo assim todo o investimento e o esforço dispendido em sua instalação.

Ao se falar sobre incidentes de segurança da informação, não se poderia deixar de citar a internet. Utilizada como o principal canal de comunicações no mundo corporativo, a rede mundial encontra-se vulnerável a uma ampla gama de ataques, não só voltados a organizações, mas também a usuários individuais. No ambiente organizacional, muitos destes ataques são de conseqüências vultosas (KORZYK SR, 1998), ou, quando não monetárias, que causam danos por vezes irreparáveis à imagem da organização, indo desde o vandalismo de "pixar" a página da empresa na internet (*site defacement*) até a retirada do ar de um ou mais servidores (*DoS* ou *DDoS*), em uma relação muitas vezes potencializada por uma mídia em geral desinformada e ávida por eventos de impacto (SCHULTZ, 2003).

4.3.2 Incidentes de segurança da informação no Brasil

A empresa de consultoria IDC apresentou no início de 2004 seu relatório "Tendências de investimento em segurança da informação no Brasil" para aquele ano (MOTTA, 2004). Foram pesquisadas 286 empresas de diversos segmentos, incluindo o Governo, tendo sido apontada uma tendência no aumento de gastos em relação ao ano anterior. Observa-se, pela Tabela 5,

que a infecção por vírus em servidores computacionais foi o incidente de maior ocorrência no período analisado, ou seja, entre fevereiro de 2003 e março de 2004.

Ocorrência	Percentual
Vírus no servidor	59
Downtime (indisponibilidade) de servidor superior a 4 horas	36
Uso não autorizado de algum sistema	24
Modificação não autorizada de dados ou configuração	18
Acesso não autorizado a informações da empresa	15
Vandalismo no conteúdo *web*	9

Tabela 5: Incidentes de segurança mais comuns no Brasil em 2003. Fonte: Motta (2004).

Em outubro de 2003 a Módulo Security Solutions S.A., a principal empresa de segurança tecnológica da informação no Brasil, apresentou os resultados de sua Nona Pesquisa Nacional de Segurança da Informação. Foram coletados 682 questionários entre os meses de março e agosto de 2003, junto a profissionais de segurança de diversos segmentos, incluindo o Governo. Dentre os resultados, pode-se salientar os seguintes (MÓDULO, 2003):

1. 42% das empresas tiveram incidentes de segurança da informação nos seis meses anteriores à pesquisa;
2. 35% das empresas reconheceram perdas financeiras devido a tais incidentes;
3. o percentual de empresas que informa ter sofrido ataques subiu de 43% em 2002 para 77% em 2003;
4. 32% dos respondentes apontaram *hackers* como responsáveis pelos incidentes reportados;
5. para 78% dos respondentes os riscos e os ataques aumentariam em 2004;
6. 48% não possuíam plano de ação formalizado para o caso de invasões e ataques;
7. 60% indicam a internet como o principal ponto de invasão de seus sistemas;
8. a falta de consciência dos executivos é apontada por 23% dos respondentes como o principal obstáculo para a implementação de segurança, enquanto 18% alegaram ser a dificuldade em justificar o retorno do investimento, 16% o custo de implementação e apenas 6% apontaram a falta de orçamento.

Quando perguntados sobre a principal ameaça à segurança da informação nas empresas, as respostas obtidas foram aquelas indicadas na Tabela 6.

Ocorrência	Percentual
Vírus	66
Funcionários insatisfeitos	53
Divulgação de senhas	51
Acessos indevidos	49
Vazamento de informações	47
Fraudes, erros e acidentes	41
Hackers	39
Falhas na segurança física	37
Uso indevido de *notebooks*	31
Fraudes em *e-mail*	29

Tabela 6: Principais ameaças à segurança da informação no Brasil em 2003. Fonte: Módulo (2003).

Ainda no Brasil, o mais citado centro sem fins lucrativos de fomento à segurança da informação, no âmbito da internet, é o *Network Information Center Security Office* - NBSO, mantido pelo Comitê Gestor da Internet no Brasil, órgão governamental com representantes da sociedade. Um demonstrativo da quantidade de incidentes relatados a este centro, no período de 1999 a 2006, é mostrado na Figura 7.
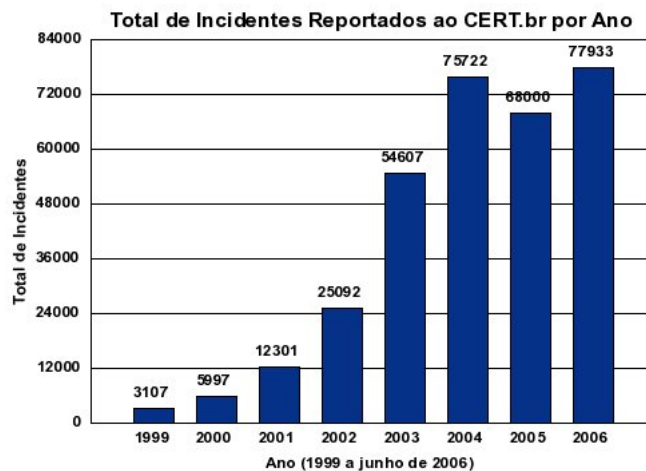
Figura 7: Incidentes reportados ao NBSO de 1999 a 2006. Fonte: NBSO (2006).

Os incidentes reportados no ano de 2005, distribuídos por tipo, estão ilustrados na Figura 8.

Outro tipo de ataque que tem se disseminado cada vez mais é o denominado *phishing*, no qual se envia uma mensagem a um grupo de usuários contendo algum tipo de atrativo, como uma suposta aprovação de crédito ou uma alegada promoção de determinada instituição comercial ou financeira, dentro da qual se insere um endereço para uma determinada página, idêntica à da instituição original, na qual se alega requerer-se um cadastramento. O usuário incauto fornece então seus dados, como a senha de acesso aos serviços bancários, que é então capturada na base
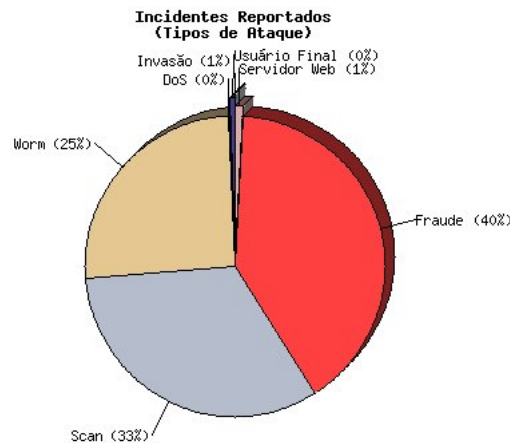
Figura 8: Tipos de incidentes reportados ao NBSO em 2005. Fonte: NBSO (2006).

de dados do atacante. De posse desta senha, para todos os propósitos, o atacante pode então se fazer passar pelo usuário, até que este verifique a ocorrência e avise a instituição correspondente.

Uma outra forma de ataque bastante disseminada é voltada às redes sem fio (*wireless networks*). Nestas redes, a conexão com servidores de acesso é feita por meio de ondas de rádio, facilitando assim a locomoção e portabilidade dos pontos de acesso. Contudo, uma vez que o éter é um bem comum, deve-se tomar cuidados especiais quanto aos parâmetros de configuração da rede, a fim de não se permitir que usuários sem a devida autorização obtenham acesso aos recursos compartilhados. Em determinados países, as instalações onde estas redes permitiam tais acessos eram sinalizadas com marcas de giz, em uma atividade denominada *warchalking*, para que *hackers* soubessem onde o acesso estaria disponível. Regras específicas de segurança têm sido desenvolvidas, voltadas a este tipo de redes (POTTER, 2003).

Nos últimos tempos, cada vez mais os usuários da internet se vêem às voltas com imensos volumes de correspondência eletrônica não solicitada, o denominado *spam*. Segundo Goodman, Heckerman e Roundthwaite (2005), cerca de um terço dos usuários da rede têm quatro de cada conjunto de cinco mensagens que lhes são enviadas originadas como *spam*. Embora não seja considerado exatamente um ataque, as mensagens não solicitadas requerem recursos computacionais e demandam tempo para o seu descarte, além de estarem diretamente associadas ao *phishing*. Diversas técnicas de prevenção a este tipo de envio vêm sendo desenvolvidas, com resultados distintos, mas, presentemente, para o usuário final, ainda resta a angustiante tarefa de fazer uma análise de suas mensagens, praticamente uma a uma.

4.4 A abrangência da segurança da informação

Embora a necessidade pela segurança da informação e os requisitos que almejam satisfazê-la estejam muito bem definidos e sejam amplamente conhecidos, conforme pode-se ver em Schneier (1996, 2000), Krause e Tipton (1999) e Alberts e Dorofee (2002), dentre outros, o estágio atual da segurança da informação assiste a um panorama no mínimo pessimista: de um lado, a engenharia de software propõe-se a desenvolver sistemas cuja aplicabilidade é medida quase que exclusivamente em termos práticos, atendendo-se a pressupostos do tipo "o sistema atende às finalidades para as quais foi concebido" [8] (PRESSMAN, 1995); de outro, assiste-se a um número cada vez maior de ocorrências de falhas de segurança relativas a sistemas de informação que não contemplaram adequadamente os conceitos da segurança em sua formulação (SCHNEIER, 2000).

A disseminação de meios maciços de acesso à informação, com a integração organizacional por meio da informática (FLORES et al., 1988) e posteriormente com a proliferação da internet e de redes corporativas, ao mesmo tempo em que introduz formas de fácil e rápida utilização dos recursos computacionais, expõe ainda mais a fragilidade e os riscos a que estão sujeitos os usuários, os sistemas e os dados armazenados e tratados por tais sistemas. Para citar-se um caso restrito ao Brasil, a iniciativa que visava à inclusão digital e que era preconizada pelo Poder Público por meio do Programa Sociedade da Informação (TAKAHASHI, 2000), aponta o foco da "segurança" como essencial ao provimento de serviços de governo [9]. O mesmo raciocínio pode ser aplicado a outras finalidades de sistemas de informação, tais como o comércio eletrônico e o acesso a páginas de instituições financeiras por meio da internet. Em todos estes casos, a preocupação com a segurança permeia os sistemas desenvolvidos, sendo item obrigatório para a sua implementação.

Entretanto, as formas correntes de implementação de mecanismos de segurança em sistemas de informação, como a criptografia, que é utilizada como prevenção ou solução para falhas em segurança na ampla maioria dos casos, são notadamente técnicas, e tendem a sê-lo em grau cada vez maior, haja vista o fato de as iniciativas apresentadas se basearem em atualizações e sofisticações da tecnologia (WOOD, 2000; SCHNEIER, 2000). Estas implementações incorporam elementos que, se não forem devidamente analisados, podem resultar em impactos negativos que se contrapõem e até mesmo anulam os benefícios alcançados, seja por não se incorporarem adequadamente aos sistemas de informação sobre os quais são implementados, seja

[8] A esta exigência, a segurança apresenta um adendo: "o sistema realiza as atividades para as quais foi concebido, e somente estas".

[9] TAKAHASHI, op. cit., p. 99

por trazerem consigo outras falhas inesperadas, por vezes maiores que as falhas que se tentava corrigir (SCHNEIER, 2000). Esta abordagem da segurança da informação termina por gerar uma série de barreiras que impedem a utilização adequada e amigável dos sistemas por parte de seus usuários.

Os mecanismos de análise e de formalização de políticas de segurança atualmente em voga, tais como a norma *International Organization for Standardization/ International Electrotechnical Commission* - ISO/IEC 17799, cuja adoção no Brasil se deu por meio da norma da Associação Brasileira de Normas Técnicas - ABNT Norma Brasileira de Referência - NBR 17799 (ABNT, 2002), ou a descrição de recomendações de institutos de tecnologia e de padrões (BASS, 1998), partem de pressupostos representados por "melhores práticas" (WOOD, 2002b), ou seja, adota-se um conjunto de procedimentos "*ad hoc*", definidos de forma empírica e exclusivamente voltados a aspectos técnicos, deslocados do contexto humano e profissional em que se inserem.

Cumpre observar que os sistemas de informação, mormente aqueles digitais, em ampla voga no contexto da Sociedade da Informação, encontram-se, naturalmente, envoltos por completo em ambientes do mundo real, estando sujeitos a várias formas de ações afeitas à sua segurança, tais como negações de serviço, fraudes, roubos, tentativas de invasão, corrupção e outras atividades hostis (SCHNEIER, 2000; WOOD, 2002a; BOSWORTH; KABAY, 2002).

Em resposta a estas hostilidades, a segurança da informação, em seu sentido mais abrangente, envolve requisitos voltados à garantia de origem, uso e trânsito da informação, buscando certificar todas as etapas do seu ciclo de vida. Estes requisitos podem ser resumidos na forma do três primeiros itens a seguir (ABNT, 2002), aos quais algumas abordagens agregam ainda os dois últimos (KRUTZ; VINES, 2002; KRAUSE; TIPTON, 1999):

Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a realizarem tal acesso (JONSSON, 1998);

Integridade: garantia de não violação da informação e dos métodos de seu processamento [10];

Disponibilidade: garantia de que os usuários devidamente autorizados obtenham acesso à informação e aos recursos computacionais correspondentes, sempre que necessário;

Autenticidade: garantia de que a informação é de fato originária da procedência alegada;

[10] É comum confundir-se integridade com corretude, mas um exemplo banal ilustra a distinção entre ambas: imagine-se uma mensagem cujo conteúdo original seja "2+2=5"; caso, ao ser transmitida, tal mensagem chegue ao seu destino com esta mesma disposição, ela mostra-se íntegra, porém, não é correta. Isto salienta também a distinção entre estrutura e significado, ao qual, conforme já se disse, a segurança não está afeita. Note-se que estes dois conceitos pertencem a domínios distintos de representação: sintático e semântico.

Irretratabilidade ou **não repúdio**: garantia de que não se pode negar a autoria da informação, ou o tráfego por ela percorrido.

Deste modo, a segurança se faz presente nas arquiteturas e modelos da informação, neles inserindo-se em todos os níveis. Entretanto, observa-se um número crescente de ocorrências de incidentes relativos à segurança da informação. Fraudes digitais, furtos de senhas, cavalos de tróia (códigos de programas aparentemente inofensivos, mas que guardam instruções danosas ao usuário, ao software ou ao equipamento), vírus e outras formas de ameaças têm se multiplicado vertiginosamente, conforme ilustra a Figura 9.
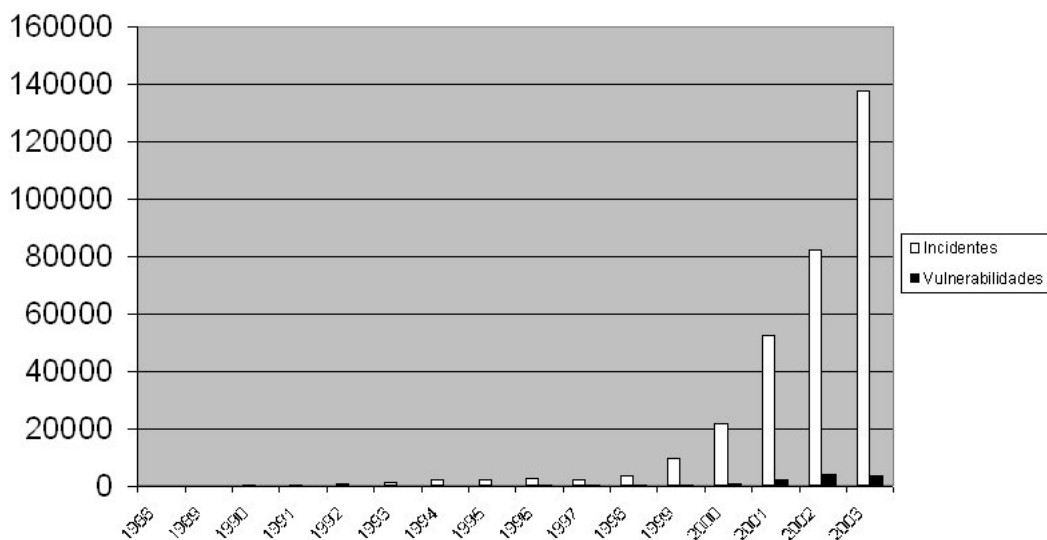
Figura 9: Vulnerabilidades e incidentes de segurança da informação em *sites* no mundo reportados no período de 1988 a 2003. Fonte: (CERT, 2004a).

Na imagem apresentada pela Figura 9, mostra-se o aumento do número de vulnerabilidades, ou seja, potenciais falhas de mecanismos computacionais (implementados em software ou em hardware), as quais, uma vez exploradas, ou em virtude de fatores não tecnológicos, como humanos, dão ensejo à ocorrência dos incidentes. Estes, por sua vez, apresentam-se em número e crescimento muito superiores às vulnerabilidades, mesmo porque a reiterada exploração de uma mesma vulnerabilidade pode ocasionar múltiplos incidentes. Observe-se, ainda, que um mesmo incidente que atinja diversas instalações (como a infecção por um mesmo vírus em centenas de milhares de computadores, por exemplo) é contabilizado como um único caso para a confecção do gráfico.A evolução destes incidentes atesta o fato de que a tecnologia por si só, da forma como vem sendo empregada, não é capaz de solucionar semelhantes problemas, levando à ocorrência de um círculo vicioso: a aplicação da tecnologia aumenta o volume de ameaças

- introduz-se mais vulnerabilidades -, às quais procura-se combater com maior aporte tecnológico. Este enfoque é resultante de uma visão canhestra da situação, que considera tão-somente os aspectos tecnológicos ali relacionados. Correntemente, para contemplar este problema a partir de uma abordagem abrangente, procede-se à adoção de estratégias organizacionais de segurança, as quais são implementadas com base em políticas de segurança institucionais.

4.5 A implementação da segurança da informação

A garantia de que os requisitos da segurança da informação serão implementados de modo adequado está intrinsecamente associada à plataforma na qual se constrói o sistema computacional em vista, seja esta plataforma construída em software, seja em hardware. Uma vez que a implementação dos requisitos em hardware atende a princípios da engenharia da construção dos componentes do sistema, estando voltada aos requisitos da engenharia deste, ela não será abordada neste trabalho. Contudo, cumpre observar que deve ocorrer a perfeita adequação entre todos os componentes do sistema a fim de garantir a segurança de todo o conjunto, uma vez que a segurança baseada em hardware tem também os seus percalços, que não são poucos e muito menos simples, como pode se ver, por exemplo, em Kocher et al. (2004).

Resta, assim, tratar sobre os componentes implementados em software, os quais, por sua vez, devem ter sua segurança implementada em dois momentos distintos, ambos na fase de especificação do sistema, qualquer que seja a metodologia utilizada, seja ela a análise estruturada, a orientação a objetos ou outras propostas, como a modelagem de ação nos sistemas de Goldkuhl e Ågerfalk (1998). Estes momentos são o levantamento dos requisitos de desenvolvimento do software e a análise do fluxo da informação ao qual este software será submetido.

4.5.1 Os requisitos do desenvolvimento de software

Pfleeger (1997) aponta para a necessidade de avaliar-se os fundamentos da segurança nos requisitos de software, a fim de garantir que as funcionalidades do sistema serão atendidas, e somente elas. O autor aponta uma lacuna em alguns padrões de qualidade de software, que, como a ISO 9126, não incluem o aspecto da segurança, e propõe que se implemente de modo continuado o aprendizado das técnicas de segurança entre os desenvolvedores, que devem ainda "pensar como o atacante" e "sempre consultar um especialista em segurança".

Carr, Tynan e Davis (1991) preconizam a segurança da informação como parte da prática de garantir a segurança do software, e cita o exemplo da *National Aeronautics and Space*

Administration - NASA no início da década de 1990, que, necessitando de software de qualidade para os seus projetos, criou e utilizou padrões de desenvolvimento que se tornaram modelos na indústria.

Wang e Wang (2003) também apontam para a necessidade de qualidade de software e segurança. Para estes autores, abordagens adequadas à segurança são feitas por meio de padrões e políticas, com o uso de bibliotecas e ferramentas de desenvolvimento e por meio da gestão administrativa do ciclo de desenvolvimento de sistemas e ferramentas físicas de manutenção.

Tryfonas, Kiountouzis e Poulymenakou (2001) salientam, do mesmo modo, que a segurança da informação deve ser inserida nas etapas de desenvolvimento de software. Os autores apontam a necessidade de um mercado global de segurança da informação e advogam que os níveis de práticas de segurança devem ser os mesmos níveis do planejamento organizacional (estratégico, tático e operacional), lembrando ainda sobre a dificuldade de uso de políticas para a efetiva segurança da informação.

Antón, Earp e Carter (2003) alertam que as políticas são independentes dos sistemas, devendo estes dois conjuntos ser harmoniosamente associados. Os autores salientam algumas abordagens aos requisitos de segurança e apresentam *frameworks* para a análise de riscos, tais como Lichtenstein (para gestão holística do risco) e PFIRES (*Policy Framework for Interpreting Risk in eCommerce Security*).

Arbaugh (2002) alerta para o fato de que elementos como o custo e a performance impedem a adequada integração dos fundamentos da segurança aos requisitos do software. Ressalta a necessidade de, em respeito à facilidade de uso, implementar-se proteção sem que ela se torne aparente ou agressiva. Um outro aspecto é lembrado por este autor: qualquer programa, não importa quão inócuo seja, pode carregar falhas de segurança. Embora a interação entre as equipes de segurança e desenvolvimento seja essencial, os profissionais da segurança não têm controle sobre o processo de desenvolvimento; logo, administram-se riscos. A fim de garantir-se o adequado acompanhamento dos requisitos de segurança, deve-se quantificar o valor da informação protegida, as ameaças àquela informação e o nível desejado de garantias. Com respeito às vulnerabilidades presentes no código dos sistemas atuais, alerta que quase 50% delas são devidas a *buffer overflow*, ou seja, acesso a endereços inválidos devido a instruções internas ao código dos programas, decorrentes de práticas inadequadas de programação.

4.5.2 O fluxo da informação

Xenitellis (2003) parte de um pressuposto bastante simples: como um sistema de software pode ser considerado um conjunto composto por código e dados, uma vez que ele não possua partes de seu código especificamente voltadas a ataques (como um cavalo de tróia), a única maneira de ele ser atacado é por meio de suas interações com o ambiente. O autor apresenta um modelo sucinto para a varredura (*tracing*) do fluxo de entrada em sistemas de software, por meio do controle de instruções de entrada e atribuições controladas pelo compilador ou por um monitor de referências de endereçamento em memória.

Zhang e Yang (2002) apresentam um modelo orientado a objetos para o controle de fluxo de entrada, baseado em controles de acesso, papéis e privilégios dos usuários envolvidos no fluxo considerado.

Chou (2004b) introduz um modelo de controle de fluxo, baseado em controle de acesso determinado por papéis (diferentes atribuições assumidas pelos componentes do sistema) voltado para sistemas orientados a objetos - *Object Oriented Role-based Access Control* - ORRBAC. O mesmo autor apresentou ainda um modelo de controle de fluxo de informações entre sistemas baseado em agentes (CHOU, 2005).

Outra modalidade de inserção de segurança em informações pode ser exemplificada pela marca d'água digital (NAGRA; THOMBORSON; COLLBERG, 2002), um processo análogo ao utilizado em documentos impressos, com a aposição de características específicas de identificação sobre o documento digital.

4.6 Aplicações da segurança da informação

As formas de aplicação da segurança da informação estão geralmente ligadas às ameaças ou vulnerabilidades identificadas ou que se deseja prevenir ou remediar. Contudo, mesmo o reconhecimento destas ameaças e vulnerabilidades não é trivial, ainda que após a ocorrência de um ataque que as explore. Korzyk Sr (1998) sugere que, em 1998, menos de 1% dos ataques era devidamente identificada e relatada, no caso da internet. Com a ampla utilização desta rede, os problemas se multiplicam de forma avassaladora. Para cada uma das formas de utilização da rede, dentre as quais algumas das principais serão mostradas a seguir, existem ameaças e vulnerabilidades correspondentes.

4.6.1 Comércio eletrônico

O volume global de negócios por meio da internet tem crescido acentuadamente nos últimos anos. Nos Estados Unidos, o comércio de bens no varejo realizado por meio da rede subiu da ordem de US$6 bilhões no ano 2000 para US$23 bilhões ao final de 2005, representando 2,4% do total de vendas gerais no varejo naquele país (US-CENSUS, 2006). No Brasil, segundo a Pesquisa Anual de Comércio realizado pelo IBGE no ano de 2003, foram movimentados R$1,85 bilhão naquele ano em transações feitas por empresas varejistas por meio da internet (IBGE, 2003). Estima-se que no ano de 2006 este volume atinja o montante de R$3,9 bilhões. As cifras envolvidas levantam diversas questões acerca dos requisitos de segurança utilizados em tais transações.

Blatchford (2000a) estima que o cadastro com informações acuradas de um único cliente potencial pode valer até US$1500,00 para um vendedor inescrupuloso. São freqüentes as ofertas de venda de listas de cadastros de endereços eletrônicos, por meio da própria rede. A conformação das organizações ao comércio eletrônico ainda está sendo comprovada à medida em que é implementada, e questões jurídicas surgem a todo instante (p. ex., em caso de disputa comercial por uma transação realizada de modo online entre duas organizações de países distintos, qual a legislação a ser aplicada? Ou ainda, numa organização que possua filiais em países distintos, como uniformizar uma política de negócios via rede?) Deve-se observar que as modalidades usadas para garantir a identidade do cliente e do fornecedor não são totalmente seguras, com a existência de fraudes sendo reportadas continuamente. Em outras palavras, o modelo de construção e implementação de comércio eletrônico está sendo posto à prova durante sua própria elaboração. Nestes casos, o aprendizado pela prática (BLATCHFORD, 2000b) pode não ser a melhor maneira de abordar o problema, com o dispêndio de recursos que se pode mostrar proibitivo, seja por razões tecnológicas, seja por razões econômicas - veja-se o grande número de falências de empresas online após o *boom* do mercado acionário no ano 2000. Nota-se uma crescente preocupação por parte dos *sites* de comércio eletrônico no sentido de tornar públicas suas políticas de segurança da informação, visando dar aos seus usuários uma ilustração de quais são as práticas ali adotadas (MCROBB; ROBERSON, 2004).

Diante desta realidade, os gestores se vêem num dilema: conectar-se à internet aumenta o risco a que estão submetidos os dados de sua organização, enquanto não integrar-se à rede pode significar perdas significativas de mercado e oportunidades de negócio. Esta realidade não se restringe ao mundo corporativo privado, mas atinge também as organizações públicas e governamentais. As soluções tecnológicas comumente adotadas apresentam limitações (HAWKINS; YEN; CHOU, 2000a) que, se não forem devidamente contempladas, podem levar a uma

situação ainda mais incômoda - a falsa sensação de segurança baseada em elementos falhos.

A necessidade de tratar as vulnerabilidades leva à adoção de novos aparatos tecnológicos, tais como a apuração e manutenção de evidências em negócios eletrônicos (SHAO; HWANG; WU, 2005), os quais, por sua vez, requerem estudos detalhados a fim de não incorrerem nas mesmas falhas dos sistemas aos quais oferecem suporte. Já se tornou evidente que a mera aplicação de recursos da tecnologia não é capaz de atender a esta demanda. A uma criteriosa análise de riscos, devem-se somar a compreensão do ambiente de negócios e a efetiva participação dos interessados (gestores, clientes, usuários) para se chegar a uma identificação mais acurada dos requisitos da segurança, que deixou de ser mero acessório para assumir papel central no contexto da informação (ZUCCATO, 2004).

4.6.2 Informação biomédica

Contemple-se a seguinte situação: o usuário coleta por meio de uma seringa uma amostra de seu próprio sangue ou de sua saliva. Insere a amostra num scanner biológico acoplado a seu computador, que envia por meio da internet os resultados da análise à clínica médica que atende àquele usuário. Em questão de minutos, o médico responsável obtém os dados da análise e prescreve a medicação e a dosagem correspondentes, enviando a prescrição, também por meio da rede, ao usuário, que em momento algum saiu de sua residência. Esta cena, que alguns anos atrás poderia compor parte de um filme de ficção científica, já é vivida em alguns países. Uma vez mais, a rede trouxe comodidade e conforto aos seus usuários. Contudo, outros acréscimos nem tão desejáveis também vieram: é preciso garantir que a amostra pertence de fato ao usuário esperado (por exemplo, no caso de moléstias incapacitantes); deve-se garantir que os dados transmitidos não sejam captados por terceiros (por exemplo, no caso de moléstias socialmente discriminadas); assim como no caso do usuário ou paciente, deve-se garantir a identidade e qualificação do médico, etc.

Observa-se que algumas destas questões não foram necessariamente introduzidas pelo uso da tecnologia, já existindo no modelo convencional da transação. Contudo, elas podem ser potencialmente amplificadas pela adoção das novas técnicas.

Tendo em vista esta realidade, organizações de saúde e de pesquisa em ciências da vida vêm adotando práticas voltadas à segurança da informação ali tratada (COLEMAN, 2004; CAVALLI et al., 2004; CPRI, 2003). Além disso, aspectos legais também já estão sendo normatizados (HELVEY et al., 2004). O impacto que estas práticas e normas trarão ao relacionamento entre usuários e organizações ou profissionais de saúde ainda é incerto.

4.6.3 Votação eletrônica

O Brasil tem se destacado como a maior democracia do mundo a utilizar votação majoritariamente eletrônica. Contudo, esta prática não está livre de problemas, como a falta de conhecimento público dos programas (software) que executam nas urnas eletrônicas e a ausência de mecanismos de recontagem de votos, para citar-se apenas o exemplo nacional.

De modo geral, os problemas que afligem a votação eletrônica são muito semelhantes aos do comércio eletrônico e aos do tratamento de informações biomédicas: a identificação segura do participante, neste caso, do eleitor. Deve-se ainda garantir que cada eleitor vote somente uma vez, ao mesmo tempo em que se garante o seu anonimato. Estes e outros problemas foram apontados por autores como Liaw (2004) e Selker (2004), e sua solução atravessa o espectro da tecnologia, a qual não os esgota: os eleitores devem se sentir confiantes quanto ao método adotado, cuja verificabilidade deve ser demonstrada.

4.6.4 Governo eletrônico

A noção de governo eletrônico carece de maior aprofundamento teórico no campo da Ciência da Informação. Quanto à sua abrangência, Lenk e Traunmüller (apud MARCONDES; JARDIM, 2003) visualizam quatro perspectivas:

1. A perspectiva do cidadão, onde visa-se à oferta de serviços de utilidade pública ao contribuinte;

2. A perspectiva de processos, onde procura-se repensar os processos produtivos existentes no Governo, em suas várias esferas, como, por exemplo, os processos de licitação para compras (o chamado *e-procurement*);

3. A perspectiva da cooperação, onde se visa à integração entre órgãos governamentais, e destes com outras organizações privadas e Organizações Não-Governamentais - ONGs, de modo a agilizar o processo decisório e a atuação destes órgãos; e

4. A perspectiva da gestão do conhecimento, onde se visa a permitir ao Governo, em suas várias esferas, criar, gerenciar e tornar disponíveis, em repositórios adequados, tanto o conhecimento gerado quanto o acumulado por seus vários órgãos.

Quanto à finalidade, Perri (apud MARCONDES; JARDIM, 2003) considera que atividades de Governo Eletrônico são as seguintes:

Fornecimento de serviços eletrônicos: área que concentra a maior parte dos esforços, recursos e atenção política voltados ao Governo Eletrônico. Caracteriza o fornecimento de serviços de utilidade pública para o contribuinte, assim como o relacionamento Governo-Empresas, usando as tecnologias da informação e comunicação que propiciam tais serviços;

Democracia eletrônica (*e-democracy*): refere-se aos sistemas de votação eletrônica e experiências piloto de consultas online aos cidadãos;

Governança eletrônica: Seria a área menos estudada do Governo Eletrônico. Inclui o suporte digital para, entre outras atividades, a elaboração de políticas públicas, a tomada de decisões, o *workgroup* entre os vários gestores públicos de diferentes escalões e o tratamento das decisões públicas e oriundas de votações ou referendos. Este tópico voltará a ser discutido no Capítulo 7.

A macro-estratégia do governo eletrônico no Brasil foi traçada no documento "A Política de Governo Eletrônico no Brasil" (PINTO, 2001), que pautava o andamento destas iniciativas no governo federal, com modificações introduzidas pela administração eleita no ano de 2002. Tal estratégia era componente do programa Sociedade da Informação no Brasil (TAKAHASHI, 2000). Associava-se a isto a iniciativa de fomento a organizações voltadas à Ciência e Tecnologia, conforme o documento conhecido como "Livro Branco" (MCT, 2002).

Modelos complementares têm sido apresentados, tais como o de Pacheco e Kern (2003), que apresenta uma arquitetura para a implementação de serviços governamentais na internet.

Nos Estados Unidos, a compreensão de que somente o governo não é capaz de proporcionar segurança ao espaço virtual ou ciberespaço (*cyberspace*), mesmo com a adoção de pesados investimentos, tais como a criação de uma rede nacional de criptografia de chaves públicas (LAMBRINOUDAKIS et al., 2003), semelhante àquela em adoção no Brasil, fez com que a política de segurança fosse endereçada ao público, reconhecendo-o como participante essencial em sua implementação.

Na Europa, modelos completos de plataformas para o provimento de serviços eletrônicos por meio do governo têm sido apresentados, sendo o mais completo o denominado SAGA - *Standards and Architectures for e-Government Applications* (SAGA, 2004), onde a segurança assume papel preponderante, sendo sugeridas diversas ferramentas. Entretanto, sendo uma plataforma tecnológica, o papel do usuário e o modelo de negócios, bem como a política governamental adotada, não são contemplados.

4.6.5 Direitos autorais

A troca maciça de informações por meio de redes, onde, uma vez mais, a internet assume papel de amplo destaque, levou a situações onde obras de arte, tais como músicas e filmes, trafegam livremente, em muitos casos à revelia de seus autores ou dos detentores de direitos autorais sobre tais peças. Embora a legislação varie grandemente entre os países (a China, por exemplo, somente reconheceu o estatuto da propriedade privada no ano de 2004), dois direitos, tidos como "morais", são via de regra reconhecidos: a autoria ou paternidade, que garante ao autor ser reconhecido como tal, e a integridade, que previne modificações em detrimento à honra ou reputação do autor. Ambos são seriamente ameaçados no contexto da internet (FERNÁNDEZ-MOLINA; PEIS, 2001).

Some-se a isto a questão da autoria de trabalhos em ambientes eletrônicos ou colaborativos, além do uso de recursos corporativos para uso particular, tais como correio eletrônico e computadores (LOCH; CONGER; OZ, 1998). Existe um imenso flanco em aberto quando se trata destas questões, que devem ser adequadamente tratadas a fim de implementar-se a segurança da informação de modo efetivo.

4.7 A gestão da segurança da informação

Ainda é usual a visão de que a gestão da segurança da informação pode ser vista como um projeto como outros, por exemplo, comerciais, no ambiente corporativo (MARTINS, 2003).

Contudo, pelo que já foi dito até aqui, pode-se ver que a segurança da informação requer atenção especial, uma vez que ela permeia todo o complexo da informação no ambiente tratado, e negligenciá-la pode até mesmo inviabilizar a execução das atividades-fim da organização.

Surgem então conceitos como a governança da segurança da informação: "conjunto de práticas e de responsabilidades exercidas pela gerência com o objetivo de prover direção estratégica, garantindo que os objetivos sejam atingidos, atestando que os riscos sejam adequadamente gerenciados e verificando que os recursos da organização sejam usados de modo responsável" (MOULTON; COLES, 2003). Este conceito será melhor explorado no Capítulo 7.

Eloff e von Solms (2000) apresentam um modelo de gestão baseado em tecnologia e processos, enquanto Eloff e Eloff (2003), por sua vez, apresentam um modelo de sistema de gestão de segurança da informação calcado em processos e padrões entronizados no ambiente organizacional, tendo em seu cerne a preocupação com as questões de caráter cultural, ético, social e legal, que são aquelas mais diretamente afeitas aos usuários.

4.8 O custo da segurança da informação

Naturalmente, a segurança da informação tem um custo. Contudo, sua ausência tem um custo ainda maior, seja econômico, seja social, na figura de uma imagem negativa perante o público.

Garg, Curtis e Halper (2003) alertam para os impactos econômicos da segurança da informação, propondo uma metodologia baseada em eventos (tipos de incidentes) para a sua análise, com reflexos sobre o valor acionário da organização em questão.

Pemble (2003) relembra a necessidade do balanceamento do orçamento voltado à segurança com os ativos que se pretende tratar: deve haver proporcionalidade entre investimentos e ativos.

Mercuri (2003) aponta a necessidade do uso de ferramentas de quantificação de custos, mesmo para as alternativas ditas como livres ou gratuitas. A autora alerta ainda para a influência de fatores culturais sobre a análise de riscos.

Gordon e Loeb (2002b) e Wood e Parker (2004) lembram que os investimentos em segurança da informação não podem ser tratados como outros tipos de investimentos. Por exemplo, a técnica de retorno do investimento (*Return on Investment - ROI*), utilizada para investimentos de caráter geral, não se aplica à segurança, pois ela não necessariamente se associa a bens tangíveis ou de retorno mensurável por medidas convencionais. Gordon e Loeb (2002a) apresentam, ainda, um modelo para a mensuração do investimento ótimo para se proteger ativos de informação, lembrando que o investimento não é necessariamente proporcional à vulnerabilidade. Lembram também que as organizações, em geral, podem investir para reduzir as vulnerabilidades, mas não as ameaças.

Gordon, Loeb e Sohail (2003) e Gordon, Loeb e Lucyshyn (2003), assim como Gordon e Richardson (2004), alertam para os custos inerentes às práticas de compartilhamento de informação, essenciais em mercados competitivos e em organizações globalizadas.

Anderson (2001) aborda diversas questões essenciais aos custos da segurança da informação, dentre os quais a opção de terceirizar-se a análise de segurança, deixando-a a cargo de especialistas, opção adotada por grande parte das organizações. Há que se observar que por melhor que seja o domínio da contratada acerca do tema da segurança, dificilmente ela terá amplo conhecimento sobre o tema do negócio da organização contratante. O autor lembra ainda o que a Economia chama de "a tragédia dos bens comuns" - quando um número elevado de usuários faz uso de determinado recurso, um a mais não faz diferença. Contudo, pode ser justamente este último a origem de uma série de problemas. Deste modo, há que se implementar soluções

por meio de regulamentação ou de aspectos culturais, e não meramente por meios tecnológicos.

O mesmo texto aborda ainda três características dos mercados de tecnologias da informação, a saber:

- o valor de um produto para um usuário depende de quantos outros usuários adotarem o mesmo produto;
- a tecnologia tem, freqüentemente, custos fixos altos e custos marginais baixos: a primeira cópia de um software ou de um chip pode custar milhões, mas as demais podem ter custos quase desprezíveis; deste modo, os bens são comercializados com base no valor e não no custo; e
- os custos associados à mudança de tecnologia são elevados, mesmo que para plataformas consideradas livres ou gratuitas.

Estas três características levam ao aparecimento de grandes monopólios de tecnologia, no modelo da Microsoft, que, por sinal, adota uma interessante forma de distribuição de produtos: realiza-se a entrega imediatamente, assim que o produto é anunciado, mas o produto só será de boa qualidade por volta da terceira versão.

Por tudo isto, o perfeito estabelecimento da diferença entre custo, preço e valor é fundamental para a determinação de políticas objetivas de investimentos em recursos tecnológicos e também em segurança da informação. Estes tópicos voltarão a ser abordados de modo mais aprofundado no Capítulo 7.

Henessy e Babcock (1998) salientam o valor da informação como elemento modificador da incerteza rumo à variabilidade conhecida.

Campbell et al. (2003) estudaram a reação do mercado ao anúncio de falhas de segurança, mostrando que as conseqüências de tais eventos podem se traduzir sobre o valor acionário da organização, principalmente quando a falha ocorrida relaciona-se à revelação de informações confidenciais.

Por fim, Rajan e Zingales (2000) alertam para "a tirania da desigualdade" em negociações onde os participantes possuem grandes diferenças de poder de negociação.

5 *Fontes de políticas de segurança da informação*

5.1 Conceitos

No sentido clássico, o vocábulo política tem sua origem no conceito de governar a cidade (*pólis*, de onde deriva *politikós*) ou o Estado, abarcando assim o que é urbano e público e mesmo o que é sociável e social, estendendo-se, posteriormente, para expressões como "ciência ou doutrina do Estado" e "ciência ou filosofia política" (BOBBIO; MATTEUCCI; PASQUINO, 1998, p. 954). Presentemente, de modo coloquial, a palavra assume por um lado um uso vago e generalizado e, por outro, um uso mais específico, no qual assume três sentidos distintos, a saber (CHAUI, 1999, pp. 368-369):

- o significado de governo, compreendido como direção e administração do poder público, constituído sob a forma de Estado. Neste sentido, a política corresponde à ação dos governantes, aos quais é conferida a autoridade necessária para dirigir a coletividade organizada como Estado;
- o significado de atividade exercida por especialistas (sejam administradores ou políticos), pertencentes a alguma agremiação ou partido, que disputam o direito de governar, exercendo cargos e postos no Estado;
- por fim, o significado, derivado do anterior, de prática duvidosa, realizada às escuras, permeada por interesses particulares e por vezes contrários aos interesses gerais da sociedade, buscando atingir fins ilícitos ou ilegítimos. Nesta acepção, é comum o uso da palavra "politicagem" para se referir a tais práticas.

Nitidamente, no contexto pretendido por este trabalho, nenhum destes sentidos do uso específico do termo será de grande ajuda. Resta o significado atribuído pelo seu uso vago e abrangente, derivado do fato de que a ampliação das ações do Estado levou também a uma ampliação

do campo das atividades políticas e sociais, que passaram a compreender questões administrativas, decisões econômicas e serviços sociais. Neste sentido, são usuais expressões como "política econômica" ou "política externa" para designar o conjunto das atividades, associadas aos seus respectivos antecedentes legais e administrativos, voltadas a atingir fins específicos na esfera indicada (econômica ou diplomática, nos exemplos citados). Em uma extensão ainda mais abrangente, o vocábulo escapou à esfera do Estado, passando à alçada organizacional ("política de marketing" ou "política de vendas") ou mesmo individual ("fulano tem por política fazer isto ou aquilo"). Enquanto nesta última construção o termo assume acepção similar a "comportamento" ou "preferência", na primeira depreende-se por "política" um conjunto de regras que se deve seguir com vistas ao objetivo estabelecido.

No que diz respeito à aplicação do termo no campo das ações de Estado (as chamadas políticas públicas), a abordagem mais usual é não definir o que o termo significa e sim tratá-lo no contexto em que se discute a abrangência da política (isto é, da iniciativa) ora sendo analisada. Embora o termo seja comumente empregado no singular, reconhece-se que, na realidade, haverá sempre a necessidade de muitas "políticas" para cobrir a complexidade de cada área (BROWNE, 1997a).

Outro conceito relacionado ao de políticas é o de **instituições**, entendidas como sendo o conjunto de procedimentos, normas, rotinas e convenções, formais ou informais, que norteiam as ações coletivas (NORTH, 1991; OSTROM, 1999, p. 36-37). Historicamente, as políticas são consideradas como pertencentes ao nível decisório coletivo das instituições, o qual é intermediário entre os níveis constitucional e operacional ou individual (KAY, 2005, p. 555).

As políticas públicas, as mais difundidas e estudadas, são vistas como o resultado de transações realizadas entre os atores políticos (órgãos do governo, agentes públicos, cidadãos, organizações públicas e privadas, entidades classistas, etc.), transações estas que são condicionadas pelas regras do jogo político e pelas ações das instituições políticas, as quais, por sua vez, dependem de características básicas de natureza constitucional e histórica (SPILLER; TOMMASI, 2003). A diferenciação entre estas bases histórico-institucionais influi diretamente sobre as políticas adotadas, podendo-se ir do sucesso na adoção de determinada política em um contexto ao fracasso da adoção desta mesma política em um contexto distinto. Características como a temporalidade (alguns países mantém as bases sobre as quais se lastreiam as suas políticas, criando assim um ambiente estável, enquanto outros apresentam alta volatilidade de ações ou de administração), adaptabilidade (alguns países são capazes de adaptar rapidamente suas políticas em resposta a variações externas ou internas, enquanto outros reagem demoradamente, mantendo políticas inadequadas por longos períodos), efetividade (enquanto alguns países têm

grande agilidade em implementar as políticas aprovadas pelo poder público, outros levam um tempo considerável em fazê-lo, ou o fazem de modo inadequado) e abrangência (em alguns países as políticas são voltadas ao interesse público, enquanto em outros privilegia-se grupos ou interesses específicos) impactam enormemente sobre o sucesso das políticas, em um mesmo continente, como a América Latina, conforme ressalta um recente relatório do Banco Interamericano de Desenvolvimento - BID, visto em Stein et al. (2005). O relatório salienta ainda a importância do processo de construção das políticas, por meio do qual elas são discutidas, aprovadas e implementadas, sobre a qualidade das políticas construídas.

Assim sendo, são fundamentais as interações entre os atores políticos, as quais têm lugar na rede política, que é uma estrutura altamente dinâmica, condicionada pelos papéis desempenhados pelos diferentes atores e pelos interesses por eles representados.

Soma-se a este panorama a constatação de que os eventos ocorridos no dia 11 de setembro de 2001 deram origem à reformulação de muitas normas e procedimentos voltados à segurança de modo geral, e à segurança da informação, em caráter particular, não só nos Estados Unidos, onde, naturalmente, este movimento é muito mais acentuado, mas também em diversas outras partes do globo.

Nos Estados Unidos, poucos dias após aquela data, criou-se o *Office of Homeland Security* (Secretaria de Segurança Interna), com status de ministério (RELYEA, 2002). Com poderes bastante abrangentes, e sem que se realizasse a discussão prévia junto à população, este órgão passou a baixar diversas normas de caráter interno e externo - os brasileiros se lembram dos episódios relativos ao cadastramento de informações de viajantes originários de outros países, como o Brasil, com destino aos Estados Unidos, o que gerou longas filas e uma iniciativa correspondente por parte das autoridades brasileiras...

Esta é um dos aspectos que se repetem com mais freqüência, no que diz respeito à segurança da informação: o estabelecimento ou o enrijecimento de medidas de segurança *depois* que algum fato relevante tenha ocorrido. No nível governamental, é comum supor-se que a segurança da informação seja tratada adequadamente pelos órgãos de inteligência e contra-inteligência destinados a este fim, inclusive com reflexos sobre a vida privada, mas nem sempre é este o caso (DESOUZA; VANAPALLI, 2005; TANAKA; MATSUURA; SUDOH, 2005). Todos, governos, organizações e sociedade, têm ainda um longo caminho a percorrer.

Outra questão de suma importância que se interpõe nesta discussão diz respeito às liberdades individuais. Estariam tais liberdades, como a do próprio acesso à informação, sendo desrespeitadas em troca da busca pela segurança em comum (SLEEMAN, 2004)? No ambiente organizacional, uma discussão acalorada diz respeito à licitude do fato de a organização

vistoriar mensagens e arquivos digitais dos empregados em busca de conteúdos considerados inadequados. Em locais como o Reino Unido esta atividade, que envolve a complexa tarefa de equacionar os direitos privados com as políticas públicas, está sendo legalizada em parâmetros considerados aceitáveis (SHARPE; RUSSELL, 2003). A análise comparada da legislação aplicada na Europa e nos Estados Unidos aponta para uma maior flexibilidade no Velho Mundo, tanto quanto às práticas adotadas como quanto à discussão das políticas junto aos parlamentos e à população (BAUMER; EARP; POINDEXTER, 2004; STRAUSS; ROGERSON, 2002). No Brasil as leis vigentes, salvo pelo Código Civil e algumas iniciativas isoladas, são muito anteriores ao evento da informatização maciça e da popularização da internet, deixando a cargo dos magistrados tomar-se as decisões cabíveis, caso atinja-se este nível.

A Organização para a Cooperação e Desenvolvimento Econômico - OCDE tem em seu *site* diversos documentos que abordam a necessidade de regulamentação adequada para a segurança da informação em seus aspectos gerais (OCDE, 2002b, 1996), além de outros específicos para transações voltadas ao comércio eletrônico (OCDE, 2001a) e privacidade (OCDE, 2001b).

Como um sistema de informações compreende tanto um sistema de processamento de dados quanto uma organização com os seres humanos que o utilizam, quaisquer políticas voltadas à informação devem se ocupar de ambos os componentes, tendo ainda em vista os objetivos organizacionais aos quais o sistema de informações deve suportar.

Um estado do sistema tal que ele atenda a todos os requisitos da política de segurança é dito um **estado seguro**. Diz-se que uma política é **consistente** se, partindo-se de um estado seguro e seguindo-se estritamente as regras ditadas pela política, não é possível atingir-se um estado inseguro.

No que diz respeito às políticas de segurança da informação, existe ainda um requisito a mais a ser cumprido: prover o equilíbrio entre funcionalidade e segurança, motivo pelo qual torna-se essencial uma análise da situação operacional da organização em foco. Esta análise, que no contexto da segurança da informação é conhecida como *análise de vulnerabilidades*, deve se restringir, como é de hábito, a uma busca por eventuais brechas de segurança nos sistemas de informação sobre os quais se aplica. Antes, deve-se conhecer a fundo os fluxos de informação aplicados (formais e informais) a fim de mapear-se de modo consistente e dinâmico a realidade, em termos da informação e dos atores que com ela interagem.

Deve-se reconhecer, ainda, que as regras ou mecanismos necessários podem não ser de fácil implementação se eles perturbam o ambiente organizacional (e isto, mesmo que em grau reduzido, geralmente ocorre). É comum encontrar-se discrepâncias entre a situação real e a situação prevista no ambiente organizacional, e as políticas de segurança devem estar prepa-

radas para lidar com esta situação. De fato, a adaptabilidade é um dos requisitos essenciais das políticas de segurança da informação, visto que os requisitos do sistema estão sujeitos a modificações. Além disso, é altamente recomendável que as políticas sejam capazes de absorver e tratar especificações existentes, mesmo que informais, mas que sejam preponderantes no ambiente organizacional.

Os elementos principais de uma política de segurança da informação são os seguintes (ORTALO, 1996):

- elementos básicos, os quais descrevem os diferentes indivíduos, objetos, direitos de acesso e atributos presentes na organização ou no sistema, e que definem o vocabulário segundo o qual a política é construída;
- os objetivos da segurança, ou seja, as propriedades desejadas do sistemas com respeito à segurança, definida em termos dos atributos desta (confidencialidade, integridade e disponibilidade);
- um esquema de autorização, na forma de um conjunto de regras descrevendo os mecanismos do sistema relevantes à segurança, com a descrição das eventuais modificações no estado da segurança.

A estrutura organizacional leva naturalmente a uma descrição estruturada de seus componentes. Os elementos básicos da política de segurança podem ser então descritos como hierarquias relacionando as várias unidades organizacionais, de modo tal que os objetivos da segurança contemplem esta hierarquização.

De modo prático, recomenda-se a construção das políticas de modo progressivo, com o uso de abstrações, como papéis a serem desempenhados: agrupando-se vários elementos sob um mesmo papel (por exemplo, cliente ou fornecedor) permite-se a adoção de conjuntos de normas relativas a cada grupo. Estas abstrações e normas são progressivamente refinadas até que se alcance um objetivo praticável e satisfatório, permitindo-se que se chegue a conclusões tais como, por exemplo, a de aplicar a apenas um grupo determinada restrição ou direito que originalmente se acreditava universal.

Alguns termos são extremamente corriqueiros no âmbito da segurança da informação, no que diz respeito à normatização e padronização das ações voltadas à segurança, sendo, por vezes, mal interpretados e utilizados fora de seu devido contexto. A fim de uniformizar a discussão no âmbito deste trabalho, cumpre realizar alguns esclarecimentos:

1. é comum a distinção dos componentes das políticas de segurança da informação de acordo com o nível organizacional em que se aplicam, dando assim origem às chamadas diretrizes (nível estratégico), normas (nível tático) e procedimentos (nível operacional) para a adoção e consolidação da segurança. Contudo, esta classificação deve-se muito mais a uma necessidade de diferenciação para termos práticos do que a uma real qualificação das fontes, formais ou informais, das regras voltadas à segurança;

2. quanto ao caráter de sua aplicação, as políticas podem ser divididas em mandatórias e discricionárias (SCHELL, 2001). A abrangência de ambas as modalidades é a mesma, variando o grau em que é aplicado e cobrado o seu acompanhamento;

3. por fim, quanto à sua formulação, as políticas também são categorizadas segundo dois tipos (CUPPENS; SAUREL, 1996): em uma política **restritiva** as informações à disposição dos usuários são exclusivamente aquelas cujo acesso lhes é expressamente permitido. Uma política **permissiva** é aquela em que são franqueadas aos usuários todas as informações cujo acesso não seja expressamente vedado. Naturalmente, a modalidade e a forma de implementação das políticas varia conforme o tipo, nicho mercadológico de negócio e a natureza da organização.

5.2 A necessidade de métricas

A necessidade de mensurar-se adequadamente os riscos a que estão sujeitas as informações em uma organização não esgota a gama de medidas afeitas à segurança. Uma vez que se implemente medidas, preventivas ou proativas, é necessário averiguar-se a sua adequação ao problema em vista. Uma pergunta que se apresenta é se a segurança da informação seria ou não adequada às mesmas práticas adotadas na mensuração da qualidade que são usadas em outros serviços de tecnologia da informação, comumente denominadas sob a expressão "concordância com o nível de serviço" (*service level agreement*) (HENNING, 2000).

Quanto a este tema, o trabalho agora apresentado propõe que a segurança seja medida por parâmetros intrínsecos à sua própria formulação, extraídos do ambiente organizacional e de seus objetivos e a eles adequados. Para tanto, propõe-se a ênfase na formulação, formalização e aplicação de políticas da segurança da informação, nos moldes descritos a seguir.

Siponen (2001) sugere que a consciência quanto à segurança da informação pode ser entendida sob cinco diferentes dimensões:

- organizacional: todos os níveis da organização, cada qual a seu modo e grau, devem ter

conhecimento da importância do tema da segurança da informação;

- pública geral: os profissionais de tecnologia da informação devem ter conhecimentos específicos sobre a segurança da informação, mas também os usuários gerais devem ter conhecimentos compatíveis com sua relação ao tema;

- sócio-política: a natureza sócio-política da tecnologia da informação deve ser devidamente tratada por aqueles indivíduos que atuam nesta esfera, tais como políticos, advogados e juristas;

- ético-computacional: a utilização ética dos recursos providos pela tecnologia da informação deve ser objeto da preocupação de todos os afeitos ao tema (pesquisadores, professores, usuários em geral); e

- educacional: deve ser preocupação constante da sociedade a adequada educação de seus membros quanto à correta e ética utilização dos recursos computacionais, inclusive com a inclusão de disciplinas curriculares nos âmbitos adequados (via de regra, os ensinamentos adquiridos limitam-se à esfera técnica).

Naturalmente, estas dimensões são ambiciosas e de imensa amplitude. No presente trabalho, propõe-se a sua conjunção com vistas ao uso consciente dos recursos providos pela tecnologia no âmbito organizacional, partindo-se do elemento mais importante do complexo da segurança da informação: o usuário.

5.3 Segurança centrada no usuário

Embora o usuário seja freqüentemente citado como o centro da atenção no tocante a sistemas de informação, a prática tem se mostrada diferente. Exemplos de sistemas desenvolvidos com pouca usabilidade ou mesmo à revelia de seus usuários não são incomuns (PRESSMAN, 1995). Sistemas ditos seguros, particularmente, são conhecidos por sua pouca amigabilidade. Zurko e Simon (1996) apresentam três categorias de aplicação da segurança centrada no usuário:

- a aplicação de testes e técnicas de usabilidade a sistemas seguros;

- o desenvolvimento de modelos e mecanismos de segurança para sistemas amigáveis (*user-friendly*); e

- a consideração das necessidades do usuário como uma meta de projeto primordial no desenvolvimento de sistemas seguros.

As políticas de segurança da informação devem enfocar estes pressupostos, de modo tal a garantir a adequação dos sistemas desenvolvidos ou adquiridos às necessidades do usuário.

5.4 Formação e conformidade

A fim de serem adequadamente desenvolvidas e aplicadas, as políticas de segurança da informação não somente devem ser vistas como o elemento de formalização das ações organizacionais quanto à segurança, mas também devem obedecer estritamente os ditames da legislação e normatização vigentes. Payne (2004) aponta algumas das vantagens da regulamentação: o aumento da segurança, o impacto econômico positivo e o aumento da atenção ao tema. O mesmo autor aponta, porém, algumas de suas desvantagens: o custo, a discordância quanto aos limites da segurança, a ausência de métricas e a extrapolação de fronteiras geográficas e sociais, principalmente no caso da internet.

Como caso de sucesso da aplicação da regulamentação quanto à segurança, o autor aponta o exemplo do chamado "bug do ano 2000" (*Y2K*), em cujo caso o alerta e a adoção de medidas pela administração pública e pelas organizações reduziram grandemente o impacto esperado pela chegada do ano 2000 sobre sistemas computacionais. O autor lembra ainda um interessante aspecto quanto à segurança da informação: quando ela funciona adequadamente, não é notada.

Legislação em excesso, porém, pode ser prejudicial. Arbaugh (2002), por exemplo, observa que a existência de leis muito amplas e vagas criou uma nuvem de incerteza quanto à pesquisa e a engenharia da segurança da informação. Com respeito à privacidade dos usuários, este tema se torna particularmente sensível (JENSEN; POTTS, 2004).

Van der Haar e Von Solms (2003) observam que as propriedades de uma organização devem determinar as metas e níveis da segurança. Os autores listam possíveis atributos para o controle da segurança, tais como os perfis dos usuários em seus diferentes níveis. Os elementos básicos do modelo proposto são:

- as propriedades da organização, tais como a natureza do negócio, propósito, ambiente, cultura, etc;
- os níveis e metas da segurança da informação, tais como confidencialidade e preditibilidade;

- os atributos de controle, como regras, auditoria e planos de recuperação de desastres, que irão acompanhar todos os controles da organização.

Pretende-se, com este modelo, proceder-se à diferenciação entre estratégias, objetivos e políticas, a fim de que cada um destes elementos seja devidamente tratado em seu nível adequado, estabelecendo-se as metas da segurança (tais como diminuir perdas e riscos, salvaguardar integridade dos dados, etc.). Os autores lembram ainda que a análise de risco é um critério subjetivo, e como tal deve ser tratada.

Outras fontes de conformidade para as políticas, além da legislação e dos princípios organizações, são os padrões propostos por organismos nacionais ou internacionais (FUMY, 2004), como os que serão discutidos mais adiante neste capítulo, e outros modelos de práticas, tais como as Request for Comment - RFC, como a RFC 2196 (*Site Security Handbook*) (FRASER, 1997) e a RFC 2828 (*Internet Security Glossary*) (SHIREY, 2000).

Torna-se patente que o desenvolvimento de políticas de segurança é um tema árduo e interminável. É preciso ter em conta que a ausência de falhas de segurança não significa que a segurança esteja sendo devidamente implementada: pode ser uma questão de tempo até que vulnerabilidades sejam exploradas. Na verdade, a tarefa do profissional de segurança é particularmente inglória: enquanto ele deve se ocupar de todas as possíveis vulnerabilidades, ao atacante basta encontrar e explorar com sucesso apenas uma delas. A própria implementação de medidas de segurança introduz novos riscos, como, por exemplo, a utilização de senhas de acesso, as quais devem ser adequadamente administradas.

Mesmo existindo padrões, a formulação e a implementação de políticas de segurança da informação ainda são feitas de modo praticamente *ad hoc* - a cada necessidade, corresponde uma política (LINDUP, 1995). Um problema particularmente grave decorre da necessidade de integrar-se políticas distintas - como garantir que as políticas componentes estejam adequadamente contempladas na política resultante (KOKOLAKIS; KIOUNTOUZIS, 2000)? Esta situação termina por levar à proposição de diversos modelos de classificação das políticas, os quais mostram-se muitas vezes inadequados (SMITH; NEWTON, 2000).

Na prática, de modo geral, contudo, as políticas tomam como passo inicial a realização de uma análise de riscos no ambiente organizacional.

5.5 Análise de riscos

A respeito da análise de riscos, que se concentra em ativos, ameaças e vulnerabilidades, Gerber, von Solms e Overbeek (2001) uma vez mais enfatizam a formalização dos requisitos de segurança da informação a partir dos requisitos do negócio.

Zhang e Yang (2002), por sua vez, salientam o fluxo da informação como determinante de sua segurança, enquanto Tsoumas e Tryfonas (2004) reforçam a importância da automação da gestão da segurança da informação a fim de dar vazão à complexidade e variabilidade dos elementos da segurança.

Diversas metodologias têm sido apresentadas para a realização de análise de riscos, em sua grande maioria proprietárias e de custo elevado de realização. Uma particularmente interessante é a denominada OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (ALBERTS; DOROFEE, 2002), desenvolvida pelo CERT no âmbito da Carnegie Mellon University e cuja documentação é de livre acesso.

A metodologia OCTAVE prevê uma ação coordenada para realizar basicamente duas tarefas:

- identificar os ativos relacionados à informação que são importantes para a organização; e
- priorizar a as atividades de análise de riscos nos ativos que forem considerados os mais críticos.

Estas tarefas, por sua vez, são desenvolvidas em três diferentes fases:

- elaboração de perfis de ameaças baseados em ativos, onde os membros da organização apresentam sua perspectiva sobre quais ativos são importantes sob a aspecto da segurança e que o está sendo feito para preservá-los;
- identificação da infraestrutura de vulnerabilidades, onde o time de analistas de segurança identifica sistemas de informação essenciais e os componentes relacionados a cada ativo, que são então analisados do ponto de vista das vulnerabilidades relacionadas; e
- desenvolvimento de planos e estratégias de segurança, onde se decide o que deve ser feito a respeito dos ativos críticos. Cria-se uma estratégia de proteção para a organização e planos voltados aos riscos dos ativos considerados prioritários.

Entre os planos elaborados na terceira fase estão o plano de recuperação de desastres e o plano de continuidade de negócios, que são componentes de virtualmente todas as metodologias de análise de riscos.

5.6 Plano de recuperação de desastres

O plano de recuperação de desastres é o documento usado para apoiar uma organização na recuperação de suas atividades de negócio, em caso de sua interrupção. Alguns dos tipos de desastres previstos são (HAWKINS; YEN; CHOU, 2000b; MIORA, 2002b) [1]:

- desastres naturais, como terremotos, tempestades, incêndios;
- mal funcionamento de software;
- mal funcionamento de hardware;
- falta de energia;
- vírus computacionais;
- ameaças humanas, como vandalismo ou sabotagem; e
- falhas humanas, como desligamento inadequado de sistemas, derramamento de líquido em computadores, etc.

Entre as vantagens da formalização de plano de recuperação de desastres estão (HAWKINS; YEN; CHOU, 2000b):

- eliminar possível confusão e erro;
- reduzir interrupções às operações da organização;
- prover alternativas durante eventos desastrosos;
- reduzir a dependência a determinados indivíduos;
- proteger os dados da organização;
- garantir a segurança do pessoal; e

[1] Compare-se esta lista com a disposta na Tabela 3.

- apoiar uma restauração ordenada das atividades.

Naturalmente, a efetivação de um plano de recuperação de desastres envolve custos, tais como a formação de uma equipe capacitada ou a contração de uma organização especializada e a preparação de mecanismos de redundância ou sobressalentes.

5.7 Plano de continuidade de negócios

O objetivo do plano de continuidade de negócios é proteger as operações da organização, e não somente seus sistemas computacionais - afinal, sem o pessoal, procedimentos em funcionamento e conectividade, não faz sentido restaurar os sistemas (MIORA, 2002a).

Em termos de perdas monetárias, um estudo empírico indicou que um sistema crítico que fique inoperante por seis dias sem uma cópia (*backup*) adequada pode gerar uma perda cumulativa de até 200% dos ganhos diários gerados pelo sistema. Após 12 dias, a perda acumulada pode atingir até 800% dos ganhos diários.

Uma análise dos ativos indica o grau de criticidade de cada um destes, o que, associado ao número de dias durante os quais a organização pode prosseguir sem o ativo considerado, gera a chamada matriz de análise de impacto nos negócios. Esta matriz é então utilizada como índice para apontar os ativos críticos e o tempo máximo suportável de indisponibilidade, orientando prioridades e investimentos.

Alguns dos padrões relacionados à segurança da informação reforçam veementemente a confecção de um plano de continuidade de negócios e de um plano de recuperação de desastres.

5.8 Organismos, leis e padrões relacionados às políticas de segurança da informação

Conforme já foi dito, as políticas de segurança da informação, para serem eficazes, devem ser aderentes à legislação e às regulamentações vigentes sobre o contexto organizacional. Leis e normas nacionais ou mesmo internacionais, além de padrões reconhecidos, contribuem para esta prática. Alguns exemplos de legislação serão discutidos a seguir.

5.8.1 Estados Unidos

Os Estados Unidos, como pólo gerador de inovações tecnológicas e como um dos país de mais alta taxa percentual de uso computacional por habitante, conforme ilustra a Tabela 7, ditam muitas das normas utilizadas pela comunidade internacional no tocante à segurança da informação. Muitas destas normas e procedimentos são gerados tendo em vista o contexto cultural e econômico daquele país, sendo criados por órgãos governamentais como o General Accounting Office - GAO (GAO, 1998) com o objetivo de embasar ou atender à sua legislação. Em outras situações, organismos de alcance global propõem e discutem modelos de normas e procedimentos a serem aplicados a todo o contexto da internet. Neste âmbito destacam-se, dentre várias organizações, o NIST, o CERT e o SANS.

País	Usuários da internet (milhões)	População (est. 2006, milhões)	Adoção da internet (%)	Parcela dos usuários no mundo (%)
Estados Unidos da América	203,8	299,0	68,1	20,0
China	111,8	1.307,0	8,5	10,9
Japão	86,3	128,4	67,2	8,5
Índia	50,6	1.112,2	4,5	5,0
Alemanha	48,7	82,5	59,0	4,8
Reino Unido	37,8	60,1	62,9	3,7
Coréia do Sul	33,9	50,6	67,0	3,3
Itália	28,9	59,1	48,8	2,8
França	26,2	61,0	43,0	2,6
Brasil	25,9	184,3	14,1	2,5

Tabela 7: Ranking de países por acesso à internet (Fonte: e-Commerce.Org (2006)).

NIST

O National Institute of Standards and Technology - NIST é uma organização voltada à normatização e padronização de instrumentos e práticas no âmbito do governo e organizações públicas nos Estados Unidos. O órgão realiza periodicamente conferências voltadas à segurança da informação, cujos resultados são publicados e disponibilizados ao público. Como exemplo, cite-se o texto de Bass (1998), o qual apresenta um modelo de política de segurança, abrangendo aspectos gerenciais, de operação e de implementação. Por sua vez, King (2000) é um texto que discorre sobre algumas das chamadas “melhores práticas” da segurança da informação, ou seja, estratégias heurísticas baseadas em casos reais, não necessariamente corroboradas pela teoria. Por fim, Raggad (2000) propõe uma estratégia de defesa corporativa, semelhante aos moldes adotados pelo Department of Defense - DoD.

CERT

O Computer Emergency Response Team - CERT (CERT, 2004b) é uma organização sem fins lucrativos, sediada na Universidade Carnegie-Mellon, na Pennsylvania, cujos relatórios es-

tatísticos anuais constituem uma referência global para o acompanhamento de vulnerabilidades, ameaças e incidentes no âmbito da internet. Além disso, o CERT realiza estudos e desenvolve instrumentos e metodologias, como a OCTAVE, citada acima, voltados ao incremento da segurança da informação, que são aplicados em larga escala, além de disponibilizar correções para falhas encontradas em diferentes softwares.

SANS Institute

O SysAdmin, Audit, Network, Security Institute - SANS Institute é uma organização de pesquisa e educação estabelecida em 1989, contando atualmente com mais de 165.000 profissionais de segurança entre seus afiliados. Além de uma grande gama de cursos e textos técnicos versando sobre a segurança da informação, o SANS Institute publicou e tornou disponíveis na internet diversos modelos *templates* de pequenas normas de segurança, voltadas a finalidades como correio eletrônico, uso de computadores, controle de acesso e muitas outras. Além disso, sua lista das 20 principais vulnerabilidades dos sistemas Windows e Unix é bastante conceituada (SANS, 2004).

Além destes textos, o SANS Institute publicou ainda um modelo para a elaboração de políticas de segurança de nível organizacional (GUEL, 2001), além de uma lista de verificação (*checklist*) para a validação da conformidade ao padrão ISO/IEC 17799 (THIAGARAJAN, 2003), que serão melhor analisados mais adiante.

DRM

Uma das principais iniciativas das grandes corporações voltadas à distribuição de conteúdos digitais voltada à segurança da informação é a proposta Digital Rights Management - DRM.

Há muita controvérsia sobre o modelo, desde que foi apresentado em meados da década de 1990. Cohen (2003) cita as restrições à privacidade: como a lei proíbe em certos casos a cópia de CDs e filmes em DVDs [2], muitos cidadãos sentem-se atingidos em seus direitos, uma vez tendo adquirido uma cópia legítima da mídia. Mas isto não é o mais controverso: o modelo prevê que os detentores dos direitos autorais recebam informações sobre o caminho percorrido por suas obras, desde a fabricação até a residência dos usuários. Alguns fabricantes de software e de hardware,principalmente os agrupados sob a Trusted Computing Platform Alliance - TCPA, como HP, IBM, Intel e Microsoft, prevêem a implementação de DRM em seus produtos (ANDERSON, 2003).

[2]Em geral, é permitida apenas um cópia como segurança, no caso de mídias voltadas à distribuição de softwares. No caso de CDs e DVDs de entretenimento a cópia é vedada.

Os provedores de conteúdo (como gravadoras e produtoras cinematográficas e de TV) alegam que as suas perdas com a pirataria justificam a implementação de mecanismos como DRM (LIU; SAFAVI-NAINI; SHEPPARD, 2003), por tratar-se de um sistema baseado em licenças digitais criptografadas integradas a um sistema de comércio eletrônico. Estuda-se a aplicação de DRM também em outras áreas, como a medicina, a fim de prover segurança aos dados do paciente.

A resistência à implementação de tal modelo vem também da comunidade científica, com críticas não somente à questão da privacidade, mas também à restrição à propagação de documentos digitais, com a alegação de que sua adoção poderia, por exemplo, impedir a disseminação e o progresso da ciência(SAMUELSON, 2003).

Também na Europa o tema suscita várias discussões, pois a União Européia cogita implementar o modelo (ARKENBOUT; DIJK; WIJCK, 2004).

Não bastassem estas considerações, há diversas críticas quanto à performance obtida pelos softwares de criptografia, que tornam mais lento o acesso aos conteúdos digitais. Diversas propostas têm surgido com o objetivo de aumentar a eficiência e acelerar o processamento dos algoritmos criptográficos (KO et al., 2005).

DMCA

Aprovada pelo Congresso dos Estados Unidos em outubro de 1998, a lei Digital Millennium Copyright Act - DMCA, voltada à proteção do trabalho intelectual (GIBBS, 2000), trouxe grande impacto sobre as atividades de muitos usuários da internet. Ela diz, em sua seção 1201, que “Nenhuma pessoa poderá ludibriar uma medida tecnológica que controle efetivamente o acesso a um trabalho protegido por esta lei” (CLARK, 2002). Deste modo, previne-se a quebra de algoritmos de criptografia, recurso muito utilizado por marginais, mas também muito comum na comunidade de usuários da rede mundial. Como exemplo, já foram enquadrados sob a DMCA usuários do algoritmo conhecido como DeCSS (*decrypt Content Scrambling System*) que permitiu a leitura de DVDs em sistemas abertos como o Linux (dos três autores do algoritmo original, postado anonimamente em uma lista na internet, dois permanecem no anonimato), e o jovem programador Shawn Fanning, criador do Napster, programa muito utilizado para a distribuição gratuita de arquivos musicais pela rede, mas que hoje encontra-se subordinado a uma aliança entre as gravadoras, provendo serviços pagos.

SDMI

A Secure Digital Music Initiative - SDMI foi proposta em apoio à DRM para o distribuição de músicas pela internet (KWOK et al., 2004), por meio de marcas d'água digitais, também baseadas em criptografia de chaves públicas. Sua implementação está em andamento, com a adesão de gravadoras como Sony, Universal e Warner.

CPRM

O padrão Content Protection for Recordable Media - CPRM foi proposta em 2001 pelos fabricantes IBM, Intel, Matsushita Electric e Toshiba, em adesão à SDMI (NETWORK SECURITY, 2001), para ser usado em dispositivos portáteis, como leitores de discos no formato ZIP e leitores de MP3. A principal novidade da proposta foi a implementação de algoritmos de segurança em hardware (GENGLER, 2001).

USA Patriot Act

Como conseqüência dos atentados terroristas ocorridos em território norte-americano no dia 11 de setembro de 2001, diversas leis e regulamentos foram aprovados ou modificados com vistas a reforçar a segurança do país contra atos de tal natureza. Uma das leis mais controversas a terem sido aprovadas foi a denominada *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* - *USA Patriot Act*, de 2002, que permite, entre outras disposições, que autoridades governamentais monitorem conversações telefônicas e por correio eletrônico de cidadãos americanos ou de cidadãos estrangeiros no país. Não tardaram a surgir alegações de que estes novos poderes estariam sendo objeto de abuso, por exemplo, sendo utilizados para espionar atividades de adversários políticas em campanhas regionais (MADSEN, 2002). A administração Bush sinaliza que pode inserir modificações na lei, tornando-a menos propensa a situações semelhantes. Outra crítica que a lei tem recebido diz respeito à retirada de informações públicas de sites governamentais, que a lei argumenta servirem como fontes de informações para eventuais terroristas. Para diversos educadores, pesquisadores e defensores da liberdade de expressão e opinião, isto representa uma séria ameaça à disseminação de tais informações, incluindo documentos históricos e já pertencentes ao domínio público (QUINN, 2003).

Em sua implementação, o *Patriot Act* introduziu modificações em diversas leis e regulamentos, indo desde a privacidade em comunicações até a regulamentação das telecomunicações, passando pelo direito de sigilo em atividades relacionadas à educação e ao crédito (JAEGER;

BERTOT; MCCLURE, 2003; REGAN, 2004). As conseqüências desta modificação no comportamento da sociedade e sua efetiva contribuição contra ações criminais ainda estão por ser devidamente observadas.

HIPAA

A lei Health Insurance Portability and Accountability Act - HIPAA, aprovada em 1996 pelo Congresso dos Estados Unidos, voltada à proteção e auditoria de dados do setor de saúde e previdência naquele país, trouxe dois movimentos principais, baseados em premissas físicas, técnicas e administrativas: uma reforma no setor de seguros de saúde, de modo tal que condições de saúde pré-existentes não se tornem impeditivas ao seguro quando da mudança de emprego, e uma simplificação administrativa, visando à redução de custos pela adoção de procedimentos padronizados de transmissões eletrônicas de dados dos pacientes (MERCURI, 2004).

Buscava-se assegurar o sigilo das informações médicas, garantindo assim a privacidade dos dados coletados, armazenados e trafegados (HELVEY et al., 2004), além de enfatizar-se a realização de ações voltadas à salvaguarda das informações (como a formulação de um plano de continuidade de negócios). Caso as prescrições da lei não sejam cumpridas, as multas previstas originalmente excedem a faixa de US$200.000 e as penas de prisão podem atingir até 10 anos. A fim de se adequar à lei, as organizações têm procedido à implementação de mecanismos e salvaguardas com vistas à manutenção da segurança das informações que tratam. A primeira data limite estabelecida para a adequação das organizações à lei foi o dia 21 de abril de 2004, sendo que este prazo foi extendido por mais 12 meses para pequenas organizações e novamente extendido por outros 12 meses para organizações de maior porte. Contrariamente ao desejado, em muitos casos, em vez de se implementar a segurança de modo adequado, introduziram-se novas vulnerabilidades, seja pelo planejamento ruim das necessidades de segurança, seja por implementações mal feitas, seja por uma combinação de ambos os eventos, associados, ainda, a um entendimento inadequado da legislação por parte de muitos pacientes e profissionais e à infra-estrutura inadequada de muitas instituições de saúde (COLLMANN et al., 2004; ALBERTS; DOROFEE, 2004). Apesar de todas as dificuldades, a lei continua em vigor, por ser considerada um passo essencial rumo à padronização de procedimentos de transmissão de dados biomédicos e à proteção da privacidade no ciberespaço.

Sarbanes-Oxley

Aprovada pelo Congresso dos Estados Unidos em 2002, na esteira de escândalos financeiros como os das gigantes Enron (energia) e Worldcom (telecomunicações), a lei Sarbanes-Oxley

estabelece várias exigências para empresas de capital aberto (que comerciam suas ações em bolsas de valores). Uma das principais exigências é de que estas empresas estabelecem e mantenham "uma estrutura de controle interno e procedimentos de relatórios financeiros adequados" (SCHULTZ, 2004).

A segurança da informação dá apoio a esta estrutura e a estes procedimentos, ao prover a confidencialidade e a integridade dos dados. Muitos gestores de segurança da informação agora vêem uma justificativa legal aos seus orçamentos: é possível determinar-se que usuário realizou que tipos de acesso a quais conjuntos de dados, gerando assim uma trilha de auditoria essencial ao cumprimento da lei e dos procedimentos realizados pelos profissionais de auditoria e contabilidade (ISACF, 2001; IT GOVERNANCE INSTITUTE, 2004b) e exigidos pelos órgãos de fiscalização - particularmente pela *Securities and Exchange Commission* - SEC, responsável pelo controle do mercado acionário no país, numa ação assemelhada à Comissão de Valores Mobiliários (CVM) no Brasil. A lei se aplica a organizações que negociam ações em bolsas de valores, inclusive empresas com sede em outros países.

5.8.2 Reino Unido

O Parlamento britânico aprovou em 1998 o *Data Protection Act*, lei que exige que as instituições voltadas para negócios de quaisquer naturezas, que detenham e usem dados pessoais, o façam de modo seguro (UK-DTI, 2004c). O padrão recomendado para a implementação de práticas de segurança da informação é o previsto pelo documento BS7799 (norma 7799 do British Standards Institute, padronizada sob a norma ISO/IEC 17799 e adotada no Brasil sob a norma NBR/17799 da ABNT). Cumpre observar que o *Data Protection Act* não se restringe a dados digitais, mas também armazenados em outras mídias.

O *UK Department of Trade and Industry* - Ministério do Reino Unido para Comércio e Indústria, criou e tornou disponível na internet uma série de publicações a respeito da lei, além de elucidar conceitos básicos sobre a segurança da informação, tais como vírus e acesso não autorizado (UK-DTI, 2004d) e sobre as implicações legais do uso de computadores e sistemas computacionais em ambientes organizacionais, tais como licenças de uso de software e a obrigatoriedade da proteção de dados (UK-DTI, 2004a).

Outra lei aprovada no Reino Unido é o *Computer Misuse Act* (UK-DTI, 2004b), de 1990, que previne o acesso e a modificação não autorizados de materiais digitais disponíveis em computador.

É importante observar que, mesmo com a existência da legislação, a adoção de políticas de

segurança em organizações no Reino Unido ainda não é uma prática usual, e mesmo as organizações que as adotam têm dificuldades em seguir os padrões propostos (FULFORD; DOHERTY, 2003).

Ainda a este respeito, May (2003) afirma que, em um estudo empírico realizado com organizações no Reino Unido, 88% dentre 150 organizações pesquisadas afirmaram que adotariam padrões de segurança da informação, mas somente 8% o faziam - a maior dificuldade citada para a implementação da BS7799 é a aceitação da alta gerência. Indivíduos ouvidos na pesquisa citaram ainda que o fato de a segurança ficar a cargo do pessoal de tecnologia da informação gera uma abordagem *bottom-up* (ou seja, iniciada nos processos de baixo nível ou operacionais da organização e deles ascendendo até os processos estratégicos) e onerosa.

5.8.3 União Européia

A consolidação da União Européia - UE e a unificação das moedas por meio do Euro criaram a virtual segunda potência econômica do mundo (BRADLEY, 2001), mas trouxeram em seu bojo uma série de desigualdades sociais, políticas e comportamentais. Além disso, o processo de consolidação da UE passa por uma série de passos voltados à uniformização de procedimentos que originalmente eram bastante distintos, embora voltados à mesma finalidade, por serem desenvolvidos e aplicados em países de culturas e históricos bastante diferentes - cite-se como exemplo a iniciativa do *Global Monitoring for Environment and Security* (GMES), que tem por objetivo a monitoração e gestão da segurança ambiental e civil (HARRIS; BROWNING, 2003). No contexto da tecnologia da informação, uma das mais prementes preocupações é a integração de bases de dados. Com o volume de informações disponível em cada país, pode-se imaginar a magnitude da tarefa a ser desenvolvida. A fim de orientar esta transição, diversos estudos foram realizados, gerando a iniciativa batizada como *"eEurope"* (EUROPEAN COMMISSION, 2002), que teve como um de seus passos mais visíveis a criação do site oficial da UE na internet, com o mesmo conteúdo disponível em cada uma das línguas dos países-membros (UE, 2003). No tocante à segurança da informação, a UE adotou um plano baseado em oito grandes programas, a saber (EUROPEAN COMMISSION, 2001):

- a formulação de políticas públicas;
- o aumento da sensibilização da população quanto ao tema, tanto no aspecto individual (EUROPEAN COMMISSION, 2003a) quanto no coletivo e no organizacional (EUROPEAN COMMISSION, 2003b);
- um sistema europeu de alerta e informações sobre segurança;

- o incremento do suporte tecnológico;
- o apoio à padronização e certificação orientadas ao mercado;
- a formação de um arcabouço legal abrangente, no qual uma das primeiras iniciativas foi a aprovação pelo Parlamento Europeu da Diretiva 95/46, que trata da proteção de indivíduos quanto ao processamento e tráfego de dados pessoais (EUROPEAN COMMISSION, 1995a), (EUROPEAN COMMISSION, 1995b);
- a aplicação da segurança pelas instituições governamentais e financeiras;
- a cooperação e parceria com países de fora da UE.

5.8.4 OCDE

A OCDE conta com a participação de 30 países membros - entre os quais o Brasil não se inclui - dentre os de economia mais desenvolvida no globo e tem sua atuação voltada para temas sociais, econômicos, educacionais e de desenvolvimento, ciência e inovação. Sediado em Paris, o organismo produz instrumentos, decisões e recomendações onde se requer a concordância multilateral entre países na esfera globalizada (OCDE, 2005). Diversos relatórios estão disponíveis no *site* da entidade e serão abordados ao longo deste trabalho, mas de antemão salientem-se aqueles voltados a ressaltar o papel da sociedade civil na formulação de políticas públicas (OCDE, 2002a; MCINTOSH, 2003; GRAMBERGER, 2001), às políticas acerca das tecnologias de informação e comunicação (OCDE, 2004) e ao combate à exclusão digital (OCDE, 2001c), bem como um mapa do uso de TI nos países-membros da entidade e no mundo (OCDE, 2002c). Destaque especial merece um relatório descritivo sobre a utilização do conhecimento para o desenvolvimento no Brasil (OCDE, 2001d), ressaltando a influente posição competitiva do país no continente e delineando uma série de sugestões para o incremento da economia nacional.

O organismo produziu para seus países-membros um guia de recomendações voltadas à orientação dos participantes em transações de dados, com vistas à criação de uma cultura de segurança em sistemas e redes de informação. Estas recomendações baseiam-se em nove princípios (OCDE, 1996):

1. atenção: os participantes devem estar alerta quanto à necessidade de segurança em sistemas e redes de informação, e quanto ao que eles (participantes) podem fazer para aumentar a segurança;

2. responsabilidade: todos os participantes são responsáveis pela segurança dos sistemas e redes de informações;
3. participação: os participantes devem agir de uma maneira oportuna e cooperativa de modo a prevenir, detectar e responder a incidentes de segurança;
4. ética: os participantes devem respeitar os interesses legítimos de outros participantes;
5. democracia: a segurança dos sistemas e redes de informação devem ser compatíveis com os valores essenciais de uma sociedade democrática;
6. análise de riscos: os participantes devem realizar análises de risco nos sistemas e redes de informação sob sua guarda;
7. delineamento e implementação da segurança: os participantes devem incorporar a segurança como um elemento essencial dos sistemas e redes de informação;
8. gestão da segurança: os participantes devem adotar uma abordagem abrangente da gestão da segurança;
9. reavalização: os participantes devem rever e reavaliar a segurança dos sistemas e redes de informação, e realizar as modificações apropriadas às políticas, práticas, medidas e procedimentos de segurança.

5.8.5 Brasil

No Brasil, somente a partir do final da década de 1990 tem-se dado importância específica a eventos da segurança da informação, no tocante aos aspectos legais e jurídicos que os envolvem. Até então, os incidentes eram enquadrados sob a óptica do contexto em que se inseriam, por exemplo, fraude ou falsificação, conforme o caso e a visão do jurista responsável.

Nos últimos anos, leis têm sido propostas para tratar especificamente de temas relacionados à segurança da informação em formato digital, como o comércio eletrônico, mas tais projetos ainda se encontram em tramitação no Congresso Nacional. A legislação brasileira, como se verá a seguir, é bastante abrangente; porém, em muitos casos, carece de atualizações essenciais à sua formalização e implementação.

NBSO

Equivalente brasileiro do CERT e principal referência nacional quanto ao tema segurança da informação na internet, o NBSO “é o Grupo de Resposta a Incidentes para a Internet brasileira,

mantido pelo Comitê Gestor da Internet no Brasil, responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet brasileira" (NBSO, 2006). Assim como o CERT em âmbito global, o NBSO disponibiliza estatísticas, cursos, textos e ferramentas relativos à segurança da informação em âmbito nacional.

Constituição Federal de 1988

Sendo a primeira Carta Magna outorgada em seguida ao término do período do governo militar (1964-1985), a Constituição de 1988 introduziu diversos dispositivos voltados à garantia de direitos individuais e coletivos, além de afiançar outros já existentes mas ainda não formalizados, como o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo a sua quebra por ordem judicial (BRASIL, 2004, Art. 5°, XII). Regulamentou-se ainda a figura do *habeas-corpus* (BRASIL, 2004, Art. 5°, LXVIII) e institui-se a do *habeas-data* (BRASIL, 2004, Art. 5°, LXXII), destinadas, respectivamente, à manutenção da integridade física e ao conhecimento do conteúdo de informações a respeito do impetrante sob a guarda do Poder Público. A aplicação deste último dispositivo, porém, é freqüentemente dificultada, como visto no exemplo da recente polêmica sobre a abertura dos arquivos relativos ao período do governo militar.

Um dos princípios essenciais da Constituição brasileira é o de que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei" (BRASIL, 2004, Art. 5°,II). Tendo em vista esta máxima, a formulação de políticas e de quaisquer outras ações coercitivas deverá se ater estritamente aos textos legais.

As disposições a respeito da implementação de tais garantias são remetidas à legislação infraconstitucional - com efeito, a expressão "privacidade" não aparece nenhuma vez no texto constitucional, enquanto o termo "segurança" é grafado duas vezes, ambas no Art. 144, destinado à descrição do aparato da segurança pública.

Código Penal - Decreto-Lei *n*° 2.840 de 7 de dezembro de 1.940

O Decreto-Lei *n*° 2.840, de 7 de dezembro de 1.940, institui o Código Penal Brasileiro - CPB (BRASIL, 1940). São muitas as discussões sobre a falta de atualização do CPB, sendo que alguns projetos de lei que visam a modificá-lo chegam a tramitar por mais de uma década no Congresso Nacional.

No tocante à segurança da informação, uma das modificações introduzidas foi a Lei *n*° 9.983, que será discutida mais adiante. Quanto às demais disposições, o CPB é considerado

por muitos juristas como anacrônico e inadequado, mas as diversas situações em que se requer sua aplicação têm sido interpretadas de modo tal a acomodar o contexto tecnológico e sócio-econômico atual.

Código Civil - Lei n° **10.406 de 10 de janeiro de 2.002**

O novo Código Civil Brasileiro (BRASIL, 2002a) ainda passa por período de adequação - o Poder Executivo extendeu até janeiro de 2.006 o prazo para que pequenas e médias organizações comerciais se adaptem aos preceitos do Código. Em seu texto, não há referências explícitas à preservação da segurança da informação.

Decreto n° **3.505 de 13 de junho de 2.000**

Este decreto estipula a Política de Segurança da Informação da Administração Federal, cujos pressupostos são os seguintes (BRASIL, 2000a, Art. 1 °):

1. assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;
2. proteção de assuntos que mereçam tratamento especial;
3. capacitação dos segmentos das tecnologias sensíveis;
4. uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;
5. criação, desenvolvimento e manutenção de mentalidade de segurança da informação;
6. capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e
7. conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Percebe-se a intenção de conciliar o princípio constitucional da inviolabilidade com a atribuição governamental da classificação e gestão de informações sensíveis. Aborda-se, ainda, o tema da capacitação dos órgãos governamentais para o uso de recursos de segurança criptográfica. O decreto cria ainda o Comitê Gestor da Segurança da Informação, formado por

representantes de doze ministérios, sendo posteriormente incluído um representante da Secretaria de Comunicação de Governo e Gestão Estratégica, com a atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional no tocante aos assuntos regulamentados pelo decreto.

Decreto n° 3.587 de 5 de setembro de 2.000

Este decreto estabelece as normas básicas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov (BRASIL, 2000b), ação governamental destinada a implementar as bases para um amplo sistema de criptografia de chaves públicas no país. Uma vez implementada, este sistema permitiria a utilização documentos digitais em substituição aos seus equivalentes impressos, com a respectiva validade jurídica.

Este decreto encontrou diversas restrições à sua implementação, por vezes de ordem tecnológica, por vezes orçamentária, por vezes jurídica, principalmente por sua complementação, dada pela Medida Provisória n° 2.200, e foi posteriormente revogado pelo Decreto n° 3.996, sendo que a ICP-Gov teve ainda seu nome mudado para ICP-Brasil.

Decreto n° 3.872 de 18 de julho de 2.001

Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CGICP-Brasil (BRASIL, 2001a). Cria-se o Comitê responsável pela gestão de políticas da ICP-Brasil.

Medida Provisória n° 2.200, de 24 de agosto de 2.001

Esta medida institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil (BRASIL, 2001c), transforma o Instituto Nacional de Tecnologia da Informação em uma autarquia federal, subordinada ao Ministério da Ciência e Tecnologia, e dá-lhe a atribuição de Autoridade Certificadora Raiz da ICP-Brasil.

Decreto n° 3.996 de 31 de outubro de 2.001

Dispõe sobre a prestação de serviços de certificação digital mo âmbito da Administração Pública Federal (BRASIL, 2001b), estabelecendo que tais serviços deverão estar subordinados à ICP-Brasil.

Decreto n° 4.073 de 3 de janeiro de 2.002 e Lei n° 8.159, de 8 de janeiro de 1991

O Decreto regulamenta a Lei n° 8.159, a qual dispõe sobre a política nacional de arquivos públicos e privados (BRASIL, 2002b), (BRASIL, 1991), dando ao Conselho Nacional de Arquivos - CONARQ a "atribuição de definir a política nacional de arquivos públicos e privados, bem como exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo" (BRASIL, 2002b, Art. 1°), além de estabelecer diretrizes para o funcionamento do Sistema Nacional de Arquivos - SINAR, que tem por finalidade "implementar a política nacional de arquivos públicos e privados, visando à gestão, à preservação e ao acesso aos documentos de arquivo" (BRASIL, 2002b, Art. 10).

Decreto n° 4.376 de 13 de setembro de 2.002 e Lei n° 9.883, de 7 de dezembro de 1999

O Decreto dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência - SBIN, instituído pela Lei n° 9.883 (BRASIL, 1999), de 7 de dezembro de 1999. Eis o que dispõe seu Artigo 1° (BRASIL, 2002c, Art. 1°):

> "§1° O Sistema Brasileiro de Inteligência tem por objetivo integrar as ações de planejamento e execução da atividade de inteligência do País, com a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional.
>
> §2° O Sistema Brasileiro de Inteligência é responsável pelo processo de obtenção e análise de dados e informações e pela produção e difusão de conhecimentos necessários ao processo decisório do Poder Executivo, em especial no tocante à segurança da sociedade e do Estado, bem como pela salvaguarda de assuntos sigilosos de interesse nacional".

Decreto n° 4.553 de 27 de dezembro de 2.002

Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (BRASIL, 2002d). Este decreto foi objeto de acalorada discussão no ano de 2005, a respeito do mecanismo de prorrogação por tempo indefinido do caráter de "ultra-secreto" de documentos.

Lei n° 9.610, de 19 de fevereiro de 1.998

Esta é a Lei do direito autoral, estabelecendo e caracterizando elementos e figuras como os diferentes tipos de obras. Caracteriza ainda os direitos morais e patrimoniais do autor (BRASIL,

1998).

Lei n° 9.983, de 14 de julho de 2.000

Esta lei altera o Código Penal, dispondo sobre a prevenção de que funcionários com acesso autorizado em alguns casos e em outros não, insiram ou alterem dados em bancos da Administração Pública (BRASIL, 2000c). Percebe-se a preocupação do legislador com a manutenção da integridade dos dados citados.

5.9 Padrões de apoio à formulação de Políticas de Segurança da Informação

A diversidade de sistemas, produtos e aplicações da informação, bem como a gama de vulnerabilidades, ameaças e incidentes, exigem a formulação de padrões da segurança - as organizações deve ter uma língua comum para a formulação dos requisitos de segurança que devem ser implementados em seus sistemas (VON SOLMS, 1999). São muitos os padrões propostos para a formulação de políticas de segurança da informação. Alguns dos mais difundidos são discutidos em seguida.

5.9.1 ITSEC

O Information Technology for Security Evaluation Criteria - ITSEC foi um dos primeiros padrões propostos para a interoperabilidade de sistemas computacionais com requisitos de segurança, principalmente criptografia de chaves simétricas. Seu desenvolvimento ocorreu como resultado de um esforço conjunto dos governos da França, Alemanha, Reino Unido e Holanda. Em meados da década de 1980, foi apresentado como um padrão proposto para a aquisição e o desenvolvimento de sistemas governamentais e comerciais (FORD, 1994). Nos últimos tempos, tem sido substituído por outros padrões, como COBIT e *Common Criteria*.

5.9.2 COBIT

Em 1998 foi criado o Information Technology Governance Institute - ITGI, organismo baseado nos Estados Unidos, com o objetivo de realizar pesquisas e estudos sobre o tema da governança, proteção e segurança de TI. Um dos principais produtos destes estudos é o guia conhecido como Control Objectives for Information and related Technology - COBIT, total-

mente compatível com a norma ISO/IEC 17799, e cujo público alvo são os gestores de organizações, auditores e responsáveis pela segurança da informação (IT GOVERNANCE INSTITUTE, 2005).

Os componentes do COBIT são os seguintes (IT GOVERNANCE INSTITUTE, 2004a):

- sumário executivo, o qual detalha os conceitos fundamentais do guia (IT GOVERNANCE INSTITUTE, 2000b);
- *framework*, que é a base e suporte para os demais componentes, organizando o modelo de processos em quatro grandes domínios (IT GOVERNANCE INSTITUTE, 2000c):
  - planejamento e organização;
  - aquisição e implementação;
  - entrega e suporte; e
  - monitoração e avaliação.
- objetivos de controle, provendo mais de 300 enunciados que definem o que precisa ser gerenciado em cada processo de TI a fim de atingir os objetivos da organização, inclusive quanto à gestão de riscos (IT GOVERNANCE INSTITUTE, 2000a);
- práticas de controle, indicando quais controles e práticas são necessários a fim de atingir os objetivos estabelecidos;
- linhas mestras de gestão, com ferramentas para dar suporte aos gestores de TI (IT GOVERNANCE INSTITUTE, 2000e); e
- linhas mestras de auditoria, delineando 34 objetivos da auditoria de TI, com atividades e um guia para a sua realização.

Além destes componentes, provê-se ainda um guia rápido (*COBIT QuickStart*) para a adoção gradual e orientada dos elementos do COBIT (IT GOVERNANCE INSTITUTE, 2000d).

5.9.3 *Common Criteria*

O projeto Common Criteria - CC é patrocinado por sete organizações de seis países distintos, a saber (NIAP, 2003a):

- Canadá: *Communications Security Establishment*;

- França: *Service Central de la Sécurité des Systèmes d'Information*;
- Alemanha: *Bundesamt für Sicherheit in der Informationstechnik*;
- Holanda: *Netherlands National Communications Security Agency*;
- Reino Unido: *Communications-Electronics Security Group*; e
- Estados Unidos: *National Institute of Standards and Technology (NIST)* e *National Security Agency (NSA)*.

O projeto foi padronizado sob o código ISO/IEC 15408. Seu objetivo é ser usado como base para avaliação de propriedades de segurança de produtos e sistemas de TI, permitindo a comparação entre os resultados de avaliações independentes de segurança, por meio de um conjunto de requisitos padronizados a ser atingidos. O processo de avaliação estabelece níveis de confiabilidade de que as funções avaliadas atingem os requisitos estabelecidos, ajudando os usuários a determinar se tais sistemas ou produtos possuem os níveis desejados de segurança e se os riscos advindos de seu uso são toleráveis. Seu público alvo são os desenvolvedores, avaliadores e usuários de sistemas e produtos de TI que requerem segurança.

O padrão está dividido em três partes (NIAP, 2003a):

- introdução e modelo geral, onde são definidos os conceitos e princípios seguidos pelo modelo, além de uma nomenclatura e uma diagramação, baseada na orientação a objetos, específicas para a formulação de objetivos de segurança, para selecionar e definir seus requisitos e para especificações alto nível de produtos e sistemas;
- requisitos funcionais de segurança, estabelecendo um conjunto de elementos funcionais para a padronização dos requisitos, divididos em classes, como gestão de segurança, privacidade e comunicação, famílias, como funções e mensagens, e componentes, como as bibliotecas de definições (NIAP, 2003b); e
- requisitos da garantia de segurança, estabelecendo um conjunto de elementos para a padronização da garantia da segurança, também divididos em famílias, classes e componentes, divididos ao longo do ciclo de desenvolvimento dos produtos ou sistemas. Um exemplo de classe é a gestão de documentação do produto ou sistema, com as famílias "guia do administrador" e "guia do usuário", contendo componentes tais como um que determine que "que o guia do administrador deve ser consistente com toda a documentação suprida para avaliação" (NIAP, 2003c).

Embora seja largamente utilizado, inclusive por organizações como a NASA e o DoD, o modelo é objeto de diversas críticas, tais como as indicadas por Schell (2001), segundo quem a ISO/IEC 15408 não responde à pergunta fundamental: “o sistema é seguro?”. Segundo aquele autor, propõe-se a criação de aplicações ditas seguras sobre uma base sem qualquer sem qualquer política claramente definida, uma vez que o modelo se preocupa exclusivamente em formalizar e avaliar os requisitos de segurança do produtos e sistemas nele baseados, mas sem observar em profundidade o ambiente em que se inserem, principalmente no que diz respeito aos recursos humanos.

5.9.4 SANS Institute

Conforme já se disse anteriormente, o SANS Institute é uma das organizações mais respeitadas no tocante à segurança da informação. Seu guia para a elaboração de políticas é simples e objetivo, tendo sido escrito numa linguagem acessível e coloquial (GUEL, 2001). Além disso, sua lista de verificação de aderência ao modelo da ISO/IEC 17799 também é bastante utilizado. O guia apresenta questões básicas de auditoria, tais como esta, obtida da seção de aderência a requisitos legais (THIAGARAJAN, 2003):

> Se controles específicos e responsabilidades individuais para atingir esta aderência foram definidos e documentados.

Além disso, diversos exemplos de normas de segurança estão disponíveis no site do SANS. Eis o exemplo de um trecho, obtido da norma sugerida para a utilização de correio eletrônico (SANS, 2002):

> Os empregados da <Nome da Organização> não devem ter quaisquer expectativas de privacidade sobre nada que eles armazenem, recebam ou enviem por meio do sistema de correio eletrônico da organização.

5.9.5 BS7799, ISO/IEC 17799 e ISO/IEC 27001:2005

Já foi visto que a norma britânica BS7799, denominada *“Code of Practice for Information Security Management”* foi ampliada e padronizada pela ISO sob o código ISO/IEC 17799, tendo sido adotada pela ABNT em 2001 sob o código NBR 17799. A aplicação de seus controles é apresentada na norma ISO 27001, publicada em outubro de 2005. A BS7799, que se baseia em outros padrões anteriormente existentes, como *Guidelines to the Management of*

Information Technology Security (GMITS) (ISO/IEC TR 13335-2, 1997), oferece diversas recomendações para os responsáveis pela gestão da segurança da informação, cujas linhas mestras devem ser delineadas em um documento da política de segurança da informação, que deverá conter pelo menos as seguintes orientações (ABNT, 2002):

- definição de segurança da informação, resumo das metas a serem atingidas e escopo a abranger;
- declaração do comprometimento da alta direção;
- breve explanação das políticas, princípios, padrões e requisitos de conformidade, tais como as relativas à legislação e à educação dos usuários;
- definição das responsabilidades gerais e específicas da gestão da segurança, incluindo o registro de incidentes; e
- referências à documentação de apoio à política.

Ainda segundo a norma NBR 17799, a disposição das políticas deve ser distribuída nas seguintes áreas (ABNT, 2002):

1. segurança organizacional;
2. classificação e controle dos ativos da informação;
3. segurança dos recursos humanos;
4. segurança física e do ambiente;
5. gerenciamento das operações de processamento da informação e de comunicações;
6. controle de acesso à informação;
7. desenvolvimento e manutenção de sistemas de informação;
8. gestão da continuidade do negócio; e
9. conformidade legal.

Torna-se patente a interdisciplinaridade exigida na formulação, apresentação, implementação e acompanhamento das políticas.

No Brasil as iniciativas no sentido de certificar-se organizações quanto a padrões de segurança ainda são incipientes, mas o Departamento de Comércio e Indústria do Reino Unido pretendia tornar a BS7799 uma exigência legal no ano de 2005 (MAY, 2003), e, ao redor do globo, a certificação de empresas no padrão ISO/IEC 17799 movimenta quantias consideráveis. Percebe-se, ao mesmo tempo, que a gestão da segurança da informação é um tema relativo à governança corporativa (POSTHUMUS; VON SOLMS, 2004; WILLIAMS, 2001). São muitos os casos de documentos tornados disponíveis por organizações de segurança da informação orientando sobre a adequação a este padrão, como os já citados produzidos pelo SANS Institute.

Um exemplo da implementação de padrões de segurança em um hospital na China é narrado por Tong et al. (2003). Os autores argumentam que para a implementação do sistema de gestão de segurança foi necessário reprojetar sistemas, modificar os fluxos de trabalho, retreinar o pessoal e implementar controles de comunicação, engenharia social e documentação.

5.10 Aplicação das Políticas de Segurança da Informação

A formulação e aplicação de Políticas de Segurança da Informação tem atingido um amplo escopo de organizações, como universidades (WALTON, 2002; FOLTZ; CRONAN; JONES, 2005) e instituições de saúde (GAUNT, 1998), tendo sido ainda objeto de estudos de órgãos governamentais (SMITH, 2001).

Os aspectos comportamentais relacionados à efetivação das políticas já têm sua importância ressaltada (MARCINCOWSKI; STANTON, 2003). Com efeito, o fato de ter-se uma disposição escrita e formalizada não significa que ela será seguida - são necessárias medidas que acompanhem a implementação das políticas, após sua implementação, mesmo em ambientes onde os usuários apresentem elevado grau de instrução, como em universidades, conforme o estudo realizado por Foltz, Cronan e Jones (2005).

Deve-se salientar, ainda, que a adequação aos padrões, principalmente os internacionais, é necessária, mas é essencial o alinhamento aos processos e ao contexto da organização (HÖNE; ELOFF, 2002a), bem como a preocupação com a clareza dos termos empregados e a proximidade com as situações vivenciadas no ambiente organizacional (HÖNE; ELOFF, 2002b).

Por sua vez, o caráter multidisciplinar das políticas de segurança da informação não decorre puramente da abrangência buscada pelo modelo adotado. Boehm-Davis (2004), entre outros, ressaltam a multidisciplinariedade advinda dos sistemas de informação, incluindo-se aí os seus usuários e projetistas. Estes sistemas são, em última instância, a origem da necessidade por requisitos de segurança que devem ser atendidos por meio das políticas.

Outro aspecto fundamental na formulação das políticas é a captação e adequação à cultura organizacional, passando por um processo de educação dos usuários às políticas adotadas, conforme é ressaltado por, entre outros, von Solms e von Solms (2004).

Um outro aspecto da multidisciplinariedade exigida pelas políticas diz respeito aos perfis necessários aos indivíduos ou organizações que as formularão, implementarão e acompanharão: deve-se ter uma formação abrangente, a fim de cobrir adequadamente todos os aspectos requeridos, além de se manter o foco nos requisitos exigidos pela gerência (WOOD, 2004).

5.10.1 A automação da gestão da segurança da informação

No Capítulo 4, falou-se da necessidade de gerir-se adequadamente os temas relacionados à segurança da informação. Vistas a abrangência e a complexidade das políticas que almejam nortear as ações organizacionais voltadas a esta segurança, advoga-se a necessidade imperiosa do uso de ferramentas de gestão adequadas para o suporte à gestão dos elementos tecnológicos, humanos e materiais envolvidos, bem como à gestão dos próprios sistemas de segurança e das políticas que regem o seu uso.

A este respeito, von Solms e von Solms (2004) apontam uma relação que denominaram "os 10 pecados capitais" da gestão de segurança da informação, a saber:

1. Não reconhecer que a segurança da informação é uma responsabilidade da alta gestão organizacional;

2. Não reconhecer que a segurança da informação é um assunto de negócios e não apenas tecnológico;

3. Não reconhecer que a governança da segurança da informação é uma disciplina multimensional, não existindo soluções prontas e acabadas capazes de atender de modo automático às mesmas demandas em diferentes contextos;

4. Não reconhecer que um plano de segurança da informação deve se basear em riscos identificados;

5. Não reconhecer ou subestimar o papel das práticas e padrões internacionais de gestão de segurança da informação;

6. Não reconhecer que uma política corporativa de segurança da informação é absolutamente essencial;

7. Não reconhecer que a adequação à segurança da informação e a sua monitoração são absolutamente essenciais;
8. Não reconhecer que uma estrutura organizacional própria para a governança da segurança é absolutamente essencial;
9. Não reconhecer a importância essencial da consciência quanto à segurança da informação junto aos usuários; e
10. Não dar aos gestores da segurança da informação poder, infraestrutura, ferramentas e mecanismos de suporte necessários ao desempenho de suas responsabilidades.

Trata-se de uma lista *"ad hoc"*, obtida da experiência pessoal dos autores, mas que se reporta a alguns dos aspectos já citados: a necessidade do comprometimento da alta gerência, da participação dos usuários e da existência de ferramentas adequadas de gestão.

Por sua vez, Vermeulen e von Solms (2002) apresentam a proposta de uma metodologia para a automação da gestão da segurança da informação, baseada em um *framework* em desenvolvimento pelos autores, semelhante ao ciclo de vida de sistemas de software e que privilegia os passos necessários à obtenção do apoio da alta gerência e da auditoria.

Skoularidou e Spinellis (2003) apresentam diferentes arquiteturas, baseados em monitores (controle automático, feito por software ou hardware, de acesso a recursos por usuários), *firewalls* e máquinas virtuais para a segurança de estações e aplicações clientes de redes.

Schneider (2000) apresenta uma proposta para a construção de mecanismos de reforço à segurança baseados em autômatos.

Fulford e Doherty (2003) realizaram uma pesquisa junto a organizações baseadas no Reino Unido, e suas conclusões apontam a necessidade de uma mais claro entendimento sobre a formulação das políticas, sua aplicação e avaliação, assim como da relação entre aplicação das políticas e a efetiva gestão da segurança da informação.

Em todos estes textos observa-se uma tendência à adoção de aspectos técnicos da segurança, enquanto não se dá ênfase ao real propósito da segurança da informação: atingir aos propósitos da organização. Em suma, é comum apresentar-se a gestão da segurança como se ela estivesse dissociada do contexto organizacional em que se insere, com todas as suas particularidades, em especial as comportamentais.

5.11 A necessidade de um novo enfoque para as políticas de segurança da informação

Muitas são as ocasiões em que as políticas de segurança da informação falham. Em várias destas, as políticas foram formuladas adequadamente, mas sua implementação se baseou em documentos e referências passivos, à espera de que os usuários viessem consultá-los. Em outros casos, a implementação já estava errada desde seus fundamentos, como a formulação (WOOD, 2000).

Esta realidade baseia-se em um pressuposto ainda mais complexo: a necessidade de uma nova definição de segurança da informação. A definição apresentada por Anderson (2003), qual seja, de que a segurança da informação é um "sentimento bem-informado de garantia de que os riscos e controles da informação estão balanceados" ainda está incompleta: deve-se cotizar a formulação dos riscos com a real percepção dos usuários, contemplar os objetivos da organização, estabelecer estratégias adequadas para a formulação, aplicação e verificação das políticas e para a sua atualização, quando necessário, como requisitos mínimos para sua efetiva adoção.

Tendo em vista estas necessidades, apresentam-se, a seguir, os fundamentos propostos para a adoção de políticas que contemplem a complexidade das interações entre os agentes sociais envolvidos na sistematização da segurança da informação.

6 A proposta da segurança da informação como um domínio multidisciplinar das ciências sociais

6.1 Interação social e comportamento

AS POLÍTICAS de segurança da informação são, via de regra, apresentadas como códigos de conduta aos quais os usuários dos sistemas computacionais devem se adequar integralmente. Entretanto, não se vê uma discussão adequada sobre o grau de receptividade a estas políticas, nem se apresentam, de modo metódico, questões sobre o impacto, usualmente considerável, por elas causado sobre o ambiente e sobre o comportamento daqueles que as devem seguir. O presente trabalho propõe que antes de apresentar-se um elemento de perturbação de uma ordem vigente (mesmo que caótica), analisem-se os indivíduos e as interações ali existentes.

O campo da interação social, o qual envolve as relações intra e interorganizacionais e portanto abarca a gênese dos sistemas de informação ali existentes, é visto pelas diferentes ciências sob vários enfoques. A Administração (BOLLOJU; KHALIFA; TURBAN, 2002) e a Economia (HENESSY; BABCOCK, 1998), por exemplo, devido à própria natureza particular dos seus objetos de estudo, debruçam-se sobre este tema com especial atenção. Desta forma, as estratégias de tomada de decisão (BOLLOJU; KHALIFA; TURBAN, 2002) e de implementação de sistemas de informação (CROTEAU; BERGERON, 2001), voltadas à geração ou à manutenção de diferenciais e vantagens competitivos, ressaltam continuamente o papel preponderante assumido pelos processos de comunicação organizacional frente aos demais processos presentes no ambiente analisado. A Ciência da Informação, por sua vez, ao ressaltar seu próprio caráter transdisciplinar e o seu relacionamento com a comunicação (“*a informação é um fenômeno e a comunicação é o processo de transferência ou compartilhamento deste fenômeno*" - (SARACEVIC, 1999)), analisa os aspectos da comunicação organizacional ora pela óptica da teoria geral dos sistemas (BATES, 1999; CHURCHMAN, 1972), ora pela óptica dos processos cognitivos

envolvidos na geração e na externalização desta comunicação (LIMA, 2003).

Do ponto de vista da Psicologia, várias abordagens aos processos da comunicação têm sido apresentadas, em particular da comunicação em ambientes organizacionais, sempre afastando-se do reducionismo materialista que caracterizou tais abordagens no decorrer do século passado, especialmente em sua primeira metade (PASQUALI, 2003). Cumpre observar que as classificações apresentadas pela Psicologia quanto aos aspectos comportamentais do indivíduo, em especial quanto àqueles manifestos em sua vida em sociedade e no âmbito organizacional, evoluíram da mera análise da intensidade dos processos neurais, tais como a excitação e a inibição na teoria de Pavlov, para conceitos mais elaborados baseados na resposta a estímulos vindos do meio, buscando identificar a estrutura da personalidade presente na resposta apresentada. Esta evolução, por sua vez, veio preencher uma lacuna da teoria da Administração quanto aos processos mais adequados para seleção e a colocação de pessoal e para o tratamento ético de empregados em situações de demissão, entre outras necessidades (GILLILAND; SCHEPERS, 2003). Um resultado evidente desta parceria é a prática adotada por muitas organizações de submeter a testes psicotécnicos os candidatos a postos de trabalho ou a promoções funcionais, muitas vezes derivando para um psiquismo exacerbado (PASQUALI, 2003), em detrimento de outras análises, por exemplo sócio-econômicas, que deveriam ser acrescidas ao conjunto de avaliações utilizadas.

Deve-se ressaltar, ainda, que cada um destes estudos atende a níveis específicos do ambiente organizacional: quando se quer observar o indivíduo e sua interações com o meio, está-se no campo da Psicologia; quando se pretende observar o comportamento de grupos diante de situações e suas ações coletivas, recorre-se à Sociologia; por fim, o estudo cultural, partindo de sua gênese e evolução, é o campo da Antropologia (BATES, 1999). Eis o motivo de propor-se uma análise da segurança da informação organizacional pela visão da teoria das ciências sociais: a informação é gerada, armazenada, tratada e transmitida com o fim de ser comunicada, e a comunicação é inerentemente um processo grupal, seja tal processo interno ou externo às fronteiras da organização.

6.2 Interação simbólica e dramaturgia social

As origens da interação simbólica remetem às obras de sociólogos como Cooley, Thomas e Mead, do final do século XIX e início do século XX. Este enfoque envolve a concepção da sociedade como um processo de interação, vendo-se o indivíduo e a sociedade como entidades intimamente inter-relacionadas. Além disso, dá-se especial atenção aos aspectos com-

portamentais do ser humano, enquanto formador e mantenedor do grupo e da identidade sociais (HAGUETE, 1995). Ao referir-se à sua própria obra, em especial ao trabalho *Mind, Self and Society*, publicada originalmente em 1934, como pertencente ao campo do "behaviorismo social", em contraposição ao behaviorismo psicológico então dominante, Mead salientava a importância do ato social não só em termos de sua componente observável, mas também da atividade não revelada, íntima, do ato. De acordo com ele, toda atividade grupal se baseia no comportamento cooperativo, diferenciando-se o comportamento humano pela *intenção* percebida nos atos dos demais atores e pela *resposta* baseada nesta percepção. Tais intenções são transmitidas por meio de gestos que se tornam simbólicos, portanto passíveis de serem interpretados, e que levam o homem a desenvolver a habilidade de responder aos seus próprios gestos. O que permite o compartilhamento de experiências e de condutas é a capacidade de diferentes seres humanos responderem da mesma forma ao mesmo gesto, desenvolvendo, assim, comportamentos grupais (HAGUETE, 1995).

As idéias de Mead foram revistas por vários pensadores, em especial Blumer, que em sua obra *Symbolic Interactionism, Perspective and Method*, de 1969, salienta aquelas que são, em seu entendimento, as três premissas básicas do interacionismo simbólico:

1. O ser humano age com relação às coisas (todos os objetos físicos, outros seres humanos, instituições, idéias, valores) com base no sentidos que elas têm para ele;

2. O *sentido* destas coisas advém da interação que o indivíduo estabelece com seu grupo social;

3. Estes *sentidos* são manipulados e modificados por meio de um processo interpretativo usado pelo indivíduo ao tratar as coisas com as quais se depara.

Deste modo, o interacionismo simbólico atribui fundamental importância ao *sentido* que as coisas têm para o comportamento do indivíduo, além de vislumbrar este *sentido* como resultante do processo de interação entre indivíduos e não como algo inato, constituinte da mente ou da psique. Deve-se observar a aproximação desta visão com os estudos fenomenológicos de Husserl e Merleau-Ponty, dentre outros (HUSSERL, 1996), e com as novas abordagens da fenomenologia aplicada à ciência da informação (MINGERS, 2001b), conforme vistas no Capítulo 3.

Essencial para o interacionismo simbólico é também o processo de auto-interação, por meio do qual o indivíduo manipula o seu mundo e constrói sua ação (HAGUETE, 1995), seja esta ação individual ou coletiva. Contrariamente à visão então vigente de que a sociedade humana

existe sob a forma de uma ordem estabelecida por meio da aderência a um conjunto de regras, normas e valores, Blumer sustenta que é o processo social de vida em grupo que cria e mantém as regras, tratando de descartar aquelas que não lhe são interessantes.

Blumer complementa que as instituições, em particular, funcionam porque as pessoas, em momentos diferentes, atuam em resposta a uma situação na qual são chamadas a agir, e não porque as organizações funcionem automaticamente em atendimento a uma dinâmica interna ou a um determinado sistema de regras e requerimentos (HAGUETE, 1995).

Baseando-se na obra de Mead, Erving Gorffman, em seu trabalho mais conhecido, *The Presentation of Self in Everyday Life*, de 1959, apresenta a importância que têm as *aparências* sobre o comportamento dos indivíduos e grupos, levando-os a agir com o intento de transmitir certas impressões aos que os rodeiam, ao mesmo tempo em que tentam controlar seu próprio comportamento a partir das reações que lhes são transmitidas pelos demais atores, a fim de projetar uma imagem distinta da realidade. A conceituação de Gorffman envolve termos como palco, desempenho, audiência, papel, peça e ato, dentre outros do vocabulário cênico. Em termos sucintos, para Gorffman, o homem é visto não como *sendo* ou *fazendo* alguma coisa, mas sim *fingindo ser* ou *fingindo fazer* alguma coisa (HAGUETE, 1995).

Considera-se que a análise dos temas acima propostos é extremamente pertinente ao âmbito da segurança da informação, uma vez que neste âmbito é comum deparar-se com o seguinte problema: implementam-se regras (freqüentemente chamadas políticas) que se mostram inadequadas ao ambiente organizacional, sendo rechaçadas pelos usuários como inadequadas, impraticáveis ou extremamente invasivas, como se vê no Capítulo 5.

6.3 A formalização de regras de conduta

Associam-se à análise realizada acima as idéias tecidas por Wittgenstein em suas *Considerações filosóficas*. Ali, ao falar sobre os requisitos necessários ao entendimento de determinado contexto social - aqui entendido como a somatória dos indivíduos e instituições resultando nas conformações observáveis -, tal como seguir determinadas regras de convívio, ele afirma que este estágio implica o conhecimento das situações subjacentes a este contexto, ou pelo menos a atenção a elas. No entanto, para Wittgenstein, o indivíduo não pode estar ciente de todos as exigências e desdobramentos do cumprimento destas regras, abrindo sempre a possibilidade de interpretações errôneas e ambíguas (TAYLOR, 1993).

Nestes termos, o próprio atendimento a regras é uma prática social, moldada pelos conceitos inerentes a cada indivíduo e traduzida pelas ações executadas em atendimento (ou não) às

regras vigentes. Conseqüentemente, a avaliação do entendimento de tais regras reside na observação das práticas adotadas, o que atribui um papel extremamente importante à compreensão do *locus* de convívio, o que se observa, por exemplo, em Heidegger (GEORGE, 2000; HEIDEGGER, 2002, 1993) e no próprio Wittgenstein (TAYLOR, 1993), e que se reflete no conceito de "habitus" (o nível de entendimento e o modo de agir social) de Bourdieu (EVERETT, 2002; MYLES, 2004; THROOP; MURPHY, 2001; GREENER, 2002a). O grau com que determinada regra é aplicada reflete a sua incorporação (*embodiment*) pelos indivíduos pertencentes ao contexto social do qual ela emana.

Outra indagação repousa sobre a forma de representação de tais regras: por mais que a interpretação seja moldada por experiências pessoais, esta representação deve se dar de tal modo que possa ser perceptível de maneira o mais uniforme possível por todos os que devem segui-la, evitando ambigüidades lingüísticas e reduzindo os mal-entendidos (inevitáveis, segundo Wittgenstein). Regras não são auto-aplicáveis nem auto-formuláveis: elas devem ser univocamente formuladas, mesmo que de modo tácito, e adequadamente aplicadas, o que exige, por vezes, uma elevada carga de julgamentos e percepções, tanto de seus formuladores quanto daqueles que se espera que as sigam, além de uma prática coerententemente alinhada com a sua formulação.

No convívio social moderno, mais especificamente na sociedade da informação, a padronização de regras de conduta voltadas ao convívio frente às fontes e acervos informacionais se traduz por meio da formulação, aplicação e acompanhamento de políticas da informação, sejam elas governamentais ou organizacionais, expressas em linguagem natural, o que as sujeita a interpretações dúbias. A fim de contornar esta dificuldade, existem propostas de representar-se as políticas de segurança da informação com base em formalismos capazes de expressar os conceitos da linguagem natural e de averiguar a consistência dos modelos ali representados, como a lógica. Esta abordagem foi, inicialmente, um dos tópicos deste trabalho, mas que foi deixada para um estudo posterior devido à complexidade envolvida na consolidação das lógicas (que chegaram a ser construídas) e pelo surgimento da questão relativa aos aspectos sócio-comportamentais do estudo.

6.4 Uma nova definição de segurança da informação

Para o objetivo deste trabalho, antes é necessária uma nova definição do que venha a ser um sistema de informações. São usuais as definições segundo as quais um sistema de informações é composto pelo complexo de tecnologia (hardware e software), enquanto outras dão um pequeno

passo adiante ao abarcar a presença do usuário. Contudo, conforme já se disse, o usuário não é um indivíduo isolado - ele vive em determinado contexto (organizacional, no interesse deste trabalho) e com ele interage, ao mesmo tempo influenciando-o e sendo por ele influenciado.

Tendo em vista estas discussões e a necessidade de uma nova abordagem de políticas de segurança da informação de caráter eminentemente social, apresenta-se a seguinte definição:

Definição 6.1 *Um **sistema de informações** é composto pela somatória do sistema social no qual ele se apresenta, ou seja, dos usuários e suas interações entre si e com o próprio sistema, e do complexo tecnológico sobre o qual estas interações se sustentam.*

Assim sendo, devem ser contemplados tanto o conjunto de elementos (software, hardware, redes) oriundos da TI e que dão suporte à realização dos sistemas, quanto os indivíduos que interagem com tais sistemas e entre si mesmos ao longo das etapas do ciclo de vida das informações ali contempladas.

Torna-se patente a necessidade não apenas da revisão do conceito da segurança da informação, mas de sua abrangência e aplicação. As modalidades de políticas vigentes visam muito mais à proteção ao fenômeno da informação, ou ao seu repositório, que ao sujeito que o presencia. Este trabalho considera que, enquanto não for estabelecido o equilíbrio adequado entre estes dois participantes privilegiados - usuário e informação, uma vez que, do ponto de vista da definição de sistema apresentada acima, um não pode subsistir sem o outro - haverá distorções de foco e, conseqüentemente, de planejamento e de implementação.

A seguinte definição procura resumir tais considerações:

Definição 6.2 ***Segurança da informação** é um fenômeno social no qual os usuários (aí incluídos os gestores) dos sistemas de informação têm razoável conhecimento acerca do uso destes sistemas, incluindo os ônus decorrentes expressos por meio de regras, bem como sobre os papéis que devem desempenhar no exercício deste uso.*

Esta definição engloba conceitos advindos de toda a discussão realizada até o momento neste trabalho: a importância das interações sociais entre os usuários de um mesmo sistema, a formação do conhecimento próprio acerca dos sistemas da informação (ou seja, do conhecimento advindo das informações obtidas do sistema e relativo a elas) e do seu uso em todas as etapas do ciclo de vida da informação, e a existência das regras de conduta relativas aos sistemas. Procura-se dar à segurança da informação um enfoque mais voltado à *proteção à*

privacidade dos usuários, diferentemente do aspecto de proteção de ativos computacionais que hoje é comumente vista.

Realiza-se em seguida uma análise do campo das políticas, do ponto de vista das ciências sociais.

7 Políticas sob a ótica das ciências sociais - gênese, novos conceitos, conformidade e aplicações

ESTE CAPÍTULO tem por objetivo apresentar uma proposta de tipologia para as políticas de segurança da informação. Antes, porém, são apresentados alguns conceitos, como a própria acepção do termo "política" conforme entendida neste trabalho, bem como uma diferenciação entre políticas públicas e ações coordenados pelo mercado no tocante à informação.

7.1 As redes de políticas públicas

As redes políticas são uma das abordagens mais utilizadas para descrever a sistemática de atuação dos agentes políticos, abarcando os aspectos informais e relacionais do ciclo de vida das políticas. Na verdade, as redes são vistas muito mais como uma metáfora da complexidade das mudanças sociais e tecnológicas do que realmente como um modelo descritivo desta complexidade. Uma desvantagem desta metáfora é que ela se apresenta altamente diversa em seu uso e mesmo em sua interpretação, sendo apontada uma necessidade de aprofundamento quanto aos conceitos apresentados (ATKINSON; COLEMAN, 1992). Contudo, isto não invalida o fato de que as redes se prestam a ilustrar a elevada dinamicidade do contexto político, sendo focalizadas, por exemplo, como uma ação coletiva em contraposição a uma visão normativa, baseada "nos manuais", dos processos envolvidos neste contexto (CARLSSON, 2000), o que se associa à constatação de que não existe um corpo de métodos ou uma metodologia abrangente para o estudo do impacto de políticas existentes como suporte a políticas futuras (RIST, 2000, p. 1001).

A gênese das redes políticas encontra-se na participação dos indivíduos em movimentos sociais e na inserção do espaço político no âmbito vital das redes sociais (PASSY; GIUGNI, 2000, 2001; EULAU; ROTHENBERG, 1986). Para Börzel (1998, p. 265), de modo qualitativo,

as redes políticas permitem a análise de formas de interação não-hierárquica entre os atores públicos e privados na construção das políticas. Outro aspecto a salientar é o de que, com a abstração das redes, cada membro é uma unidade independente, o que impossibilita o uso do poder de modo unilateral, uma vez que o poder informal baseado nas relações interpessoais pode ser mais importante que o poder formal (KEAST et al., 2004, p. 365). De modo bastante significativo, também nos contextos tecnológico e econômico a metáfora das redes tem sido cada vez mais utilizada para descrever as relações humanas, como se vê, por exemplo, em Castells (2003).

A dinamicidade da metáfora ganha mais ênfase ao se constatar que a configuração da rede pode variar conforme o tema e a política sob observação. Associadas às redes estão as comunidades, visto que, enquanto o universo político compreende todos os agentes que têm algum interesse em comum, a comunidade política é uma rede menor e mais consensual que se focaliza em um aspecto setorial ou mesmo sub-setorial da política. As comunidades interagem em uma rede (PARSONS, 2001, p. 189). Uma visão da diferenciação entre comunidades e redes é mostrada na Tabela 8.

Critério	Comunidades	Redes
Interação entre os participantes	Alta	Baixa
Integração ao processo de implementação das políticas	Alta	Baixa
Abrangência dos temas de interesse	Baixa	Alta
Participação do estado	Estado dependente de grupos para a implementação das políticas. Os grupos de interesse têm recursos importantes para trocar.	Áreas menos importantes para o estado, de alta controvérsia política ou áreas nas quais os interesses ainda não foram institucionalizados.

Tabela 8: Comunidades e Redes políticas. Adaptada de Parsons (2001, pg. 190) e Blom-Hansen (1997, p. 671).

Um outro conceito relacionado às redes e às comunidades é o das coalisões de advocacia, onde o processo de estabelecimento da agenda política é dominado pelas opiniões de uma elite, orientada por suas crenças e preferências e exercendo amplamente seu poder de veto, enquanto o impacto da opinião pública é no máximo modesto. Em cada subsistema político, há uma multitude de coalisões, competindo pela influência sobre o processo decisório (SABATIER, 1991, p. 148), e às quais se opõe a estrutura institucional ou organizacional dos órgãos públicos ou entidades privadas de representação, que procuram equilibrar este jogo. Exemplo recente e bastante próximo desta atuação diz respeito ao processo de votação da chamada “MP do Bem” (sancionada sob a Lei n° 11.196/2005), onde conflitos entre comunidades e coalisões ficaram

patentes, inclusive internamente à esfera governamental.

Associe-se a isto o fato de que as políticas, assim como as instituições, têm uma grande tendência à inércia. Uma vez que os fundamentos para as políticas são estabelecidos, exige-se um grande esforço para a sua modificação e aqueles mesmos fundamentos irão constituir-se em restrições para atividades futuras (GREENER, 2005, p. 62). Uma outra faceta desta acomodação gera impactos diretos sobre as escolhas tecnológicas, onde, por exemplo, a atualização de determinados padrões que com o tempo se mostram obsoletos encontra enormes obstáculos. Um exemplo clássico é o do dos teclados no padrão QWERTY, mesmo tendo sido mostrado por estudos realizados na década de 1940 que o custo da substituição pelo padrão Dvorak, muito mais eficiente, seria coberto em apenas dez dias (GREENER, 2002b, p. 614). Uma das teorias voltadas a explicar esta tendência é a chamada dependência do caminho (*path dependency*), a qual se relaciona pelo lado tecnológico, para citar-se dois exemplos de grande relevância atual, com a grande resistência enfrentada na adoção de padrões abertos de software (JAMES, 2003) e com a lentidão na atualização de versões do sistema operacional Microsoft Windows (LOHR; MARKOFF, 2006).

Naturalmente, isto não quer dizer que o futuro das políticas esteja determinado já em seu nascimento. Pelo contrário. Do lado institucional, diversos organismos, tais como OCDE, FMI, União Européia e Banco Mundial propõem a padronização e a uniformização de procedimentos para a formalização e a adoção de políticas públicas, mas já se sabe a vasta dependência destas em relação às instituições (representadas pelas redes e comunidades) e ao mesmo tempo ao encadeamento histórico percorrido, sendo muitos os exemplos que ilustram o insucesso da adoção de modelos bem sucedidos em outros contextos, como a reforma previdenciária no Brasil (MELO, 2004).

Outra questão que se impõe diz respeito às relações de causalidade na formulação das políticas: seriam elas o resultado da interação entre os diferentes atores políticos no ambiente em que se encontram, ou seria a própria ação das políticas o que molda estas interações? Em outras palavras, quais seriam as relações mais preponderantes associadas à natureza das políticas? Embora uma relação de causa-efeito não seja universalmente clara, existindo exemplos apontando em ambas as direções, a ausência de uma resposta objetiva não se constitui, naturalmente, em um obstáculo à formulação e à aplicação das políticas (PASSY; GIUGNI, 2001; SPILLER; TOMMASI, 2003; DAVIES, 2000).

Os críticos da dependência do caminho apontem que ela se restringe a explicar a estabilidade e não a mudança. De qualquer modo, ela deve ser entendida mais como uma categoria empírica do que uma teoria de fato, uma vez que carece de maiores fundamentos por não prover

os meios ou condições necessários ao correto entendimento dos fenômenos que aponta (KAY, 2005). Mas isto não invalida o fato de que os sistemas políticos, compreendendo as redes e as comunidades, são de baixa preditibilidade, ao menos no curto prazo, possuindo propriedades emergentes de acordo com as variadas possibilidades históricas identificadas em seu nascedouro e que são determinadas ao longo de sua existência (ORMEROD, 2005).

Mediante o acima exposto, observando-se as interações necessárias para a formulação das políticas, tanto no nível estatal quanto no nível organizacional, apresenta-se o conceito adotado neste trabalho, sintetizado na definição apresentada a seguir, derivada de Schmitter (1982, p. 34):

Definição 7.1 *Uma* ***política*** *é uma linha de conduta coletiva, resultante da interação entre atores dentro de um quadro de cooperação-integração reciprocamente reconhecido. Nestes termos, é um fenômeno eminentemente social e como tal deve ser compreendido.*

Amplamente, são as políticas de caráter público as mais estudadas, tanto por sua relevância quanto por seu número e formas de disseminação. Contudo, é extremamente importante ressaltar a relevância da regulação implementada pelo mercado, na forma de regulações competitivas, ou seja, submetidas à competição expressa em termos de demanda por parte dos usuários. Embora em muitos casos a ação do governo se faça essencial, em vários outros casos ela se mostra, uma vez observada a sua atuação ao longo do tempo, danosa e contraproducente, como ilustra muito bem o exemplo da reserva de mercado adotada no Brasil, durante o regime militar, para os softwares e componentes de informática (ROSENBERG, 1982). Neste exato momento, um outro exemplo é vivido novamente pelos brasileiros: a escolha do padrão de televisão digital, quando já se apresenta a preferência do poder público sem que se façam discussões adequadas dentro da sociedade e quando o próprio modelo escolhido não atinge consenso dentro do grupo de ministros de estado envolvidos com a escolha. Por outro lado, no contexto externo, sérias críticas são feitas ainda ao modelo de regulamentação adotado quanto aos direitos autorais e direitos de cópia de conteúdos dispostos em mídias digitais, já discutidos na Seção 5.8, onde as empresas produtoras dos conteúdos ditam a regulamentação que é adotada (ELKIN-KOREN, 2001). O modelo misto de privatização em seguida à regulamentação, com arbitragem por parte de uma agência independente, adotado no Brasil para o setor de telecomunicações, entre outros, é visto como bem-sucedido, funcionando como um paliativo para a presença excessiva do estado (KAPLAN; CUCITI, 1998), equilibrando as diferenças (tempo de reação, recursos disponíveis, poder de coerção, tolerância a riscos) entre o mercado e o poder público (NUTT, 2005; CHRISTENSEN; PALLESEN, 2001).

Particularmente no que diz respeito à segurança da informação, existe um complicador: como conciliar a necessidade da privacidade e dos direitos individuais com o interesse público, o que gera conflitos de diversas magnitudes, como a supervisão de mensagens de correio eletrônico por parte da organização, por exemplo (SHARPE; RUSSELL, 2003).

7.2 A governança e as redes corporativas

Embora seja um lugar-comum diferenciar-se as organizações governamentais das privadas e não-governamentais com base na aferição de lucros, deve-se salientar que a visão e o tratamento dos conceitos relacionados à informação não apresentam diferenças marcantes. O que difere é o uso destes conceitos com vistas aos objetivos estabelecidos. No mundo corporativo, é comum a introdução do conceito da governança corporativa para sumarizar os estamentos aos quais a organização deve se sujeitar. Enquanto pelo lado do governo o termo governança aplica-se ao processo pelo qual a sociedade gere a si mesma (UNESCO, 2002), no lado corporativo a governança é comumente vista como um contrato entre os *shareholders* (representados pelos acionistas) e os agentes (*stockholders*, representados por um quadro de gerência ou pela figura individual do CEO (*chief executive officer*)) (TIROLE, 2001), com atenção especial voltada às estruturas de monitoramento e controle externo e interno responsáveis pela execução deste contrato (SCHMIDT; SPINDLER, 2002). Há diversos estudos dedicados aos diferentes tipos de governança encontrados, tais como o de Weimer e Pape (1999), que analisa os estilos caracterizados como anglo-saxão, germânico, latino e japonês, ou o de Ryan (2005), que analisa a ética nos negócios e a gestão corporativa nos três países da América do Norte, ou o de Alves e Mendes (2004), realizado em Portugal.

É reconhecida a necessidade de maiores fundamentos teóricos para analisar-se adequadamente as ferramentas e modalidades de gestão corporativa, citando-se como exemplo o trabalho de Turnbul (2002), que sugere a aplicação da TBA - (*Transaction Byte Analysis*), uma técnica baseada na teoria da informação de Shannon, vista na Seção 2.2.2, para a metrificação do fluxo da informação entre os diferentes atores no processo de governança corporativa. O trabalho de Ayogu (2001, p. 309) acerca da governança corporativa na África introduz uma observação fundamental:

> Do ponto de vista prático, o problema da governança corporativa está relacionado ao delineamento de instituições que orientam o corpo de gerentes em suas ações, de modo tal a levar em consideração o bem-estar dos *stakeholders* - investidores, empregados, comunidades, fornecedores e clientes.

Deste modo, a governança corporativa assume o papel de delinear as fronteiras da ação do

corpo gestor frente aos demais atores, representando um conjunto de instituições, mormente um corpo de políticas e de regras, capaz de coordenar esta ação. Particularmente no que diz respeito à segurança da informação, privilegiam-se os aspectos de responsabilidade e transparência, conforme se vê, por exemplo, em Williams (2001), ISACF (2001) ou em Posthumus e von Solms (2004) - o Capítulo 5 apresenta uma coletânea de estudos e proposições acerca da governança da segurança da informação.

Tanto no aspecto governamental quanto no "mercado" a informação apresenta uma outra característica essencial, a chamada exterioridade de rede ou efeito de rede: o valor (monetário ou não) de ligar-se a uma rede depende do número de outras pessoas já conectadas a ela (SHAPIRO, 1999, p. 205), asserção associada à chamada "Lei de Metcalfe", segundo a qual o valor da rede é proporcional ao quadrado do número de seus participantes (SHAPIRO, 1999, p. 216). Ou seja, quanto mais extensas forem as conexões criadas ou permitidas pela rede, maior será o interesse de outros atores em participar dela, o que, por um lado, impulsiona as redes de grande extensão a se tornarem ainda mais abrangentes, mas, por outro lado, tem um efeito nefasto sobre as redes pequenas - elas têm uma probabilidade muito pequena de florescerem, razão pela qual a introdução de novos conceitos (como a adoção de procedimentos voltados à segurança da informação) requer uma cuidadosa estratégia de apresentação e de adoção.

Esta análise leva a uma constatação determinante para a gênese das iniciativas organizacionais: a governança corporativa e a gestão dos recursos informacionais como um todo não podem ser independentes da governança pública e das políticas públicas que a determinam, mais um dos motivos por que estas políticas devem assumir a merecida relevância.

7.3 Políticas públicas

A principal preocupação das políticas públicas consiste em como definir e desenvolver questões e problemas de modo tal a que eles sejam inseridos na agenda pública e política (PARSONS, 2001, p. xv). Esta orientação compreende um processo multimetodológico, multidisciplinar, com clara ênfase nos problemas tratados e voltado a mapear o contexto do processo político, as opções de ação existentes e os resultados delas advindos, na visão de Lasswell (PARSONS, 2001, p. xvi).

Historicamente, o conceito e a aplicação das políticas públicas evoluiu da visão platônica segunda a qual as políticas deveriam prover os meios para que as esferas pública e privada pudessem ser balanceadas, passando pela concepção pós-*New Deal* de que o papel do estado deveria se restringir à gestão da *res publica*. Posteriormente, o conceito sofreu influência dos ideais

liberais, de que o mercado voltaria a ditar os caminhos da sociedade, por meio dos princípios de gestão equilibrados por conceitos monetários e de propriedade, até chegar aos tempos atuais, onde se vê, em muitos casos, uma franca incapacidade dos poderes públicos no provimento de serviços essenciais e, em outros, a presença do estado sendo provida por meio de mecanismos digitais característicos da Sociedade da Informação - não raro, ambas as situações ocorrem em um mesmo país. Neste contexto, as políticas públicas representam as meta-escolhas, ou seja, as escolhas realizadas em qualquer que seja a esfera da intervenção da autoridade pública (HECLO, 1972).

O uso crescente e disseminado de recursos tecnológicos, não somente os voltados à informação em si, mas também em outras áreas, como a biologia (com novas áreas como a proteômica e a engenharia genética) e a ciência dos materiais (com a nanotecnologia e a supercondutividade), impõe a adoção de estratégias capazes de determinar os rumos a serem adotados em tais campos do conhecimento, tanto por parte de órgãos e agências governamentais quanto por organizações privadas e mistas. Estas estratégias têm seu delineamento explicitado por meio das políticas, as quais devem ser claras, de modo a serem compreendidas e seguidas, e flexíveis, de modo a permitir alterações requeridas por necessidades de qualquer ordem pertinente (social, política ou econômica, inclusive com a mudança de modelos, tais liberal ou estatizante, etc) (WILSON, 2000; CHRISTENSEN; PALLESEN, 2001). Assim, as conseqüências sociais da aplicação destas políticas, mormente as governamentais ou públicas, atinge um amplo espectro, motivo pelo qual sua formulação e aplicação são objetos de ações de planejamento estratégico especificamente voltadas a garantir o seu sucesso - o que nem sempre se consegue.

À parte as questões relacionadas à finalidade das políticas (por exemplo, na formulação de leis e estatutos jurídicos, onde a prática consiste em um *savoir faire* por vezes sem conexão com a análise empregada em sua formulação) o ciclo elaboração-ação-avaliação-intervenção é a tônica na formulação e aplicação de políticas públicas e, por extensão, organizacionais (SHULOCK, 1999; GERSBACH, 2000; BUSENBERG, 2001). A fim de lidar com os volumes de informação requeridos, utilizam-se, obviamente, recursos tecnológicos, o que ocasiona a geração de um paradoxo: faz-se uso extensivo de um recurso cuja utilização se está normatizando. Esta situação se torna ainda mais patente quando se requer a aplicação de ações envolvendo diferentes países, como o arbitramento de questões jurídicas como patentes e jurisdições - o *site* de uma organização norte-americana, que está instalado em um servidor computacional localizado na Alemanha e atende a clientes no Japão está sujeito à legislação de qual país? Da mesma forma, com as novas possibilidades de ativismo social, político e econômico, um usuário dinamarquês que utilize um *site* baseado na Inglaterra para realizar um ataque computacional a uma empresa canadense deverá ser enquadrado sob qual legislação?

Uma das questões tratadas neste escopo é o de uma governança global voltada a temas relacionados às tecnologia da informação e de comunicação, com o incremento das relações entre governo e cidadãos, especialmente no acesso às informações providas por órgãos de governo, sem perder de vista as necessidades locais (ROSE, 2005; HUDSON, 2003; HITCHENS, 1997; BLOM-HANSEN, 1999). São gritantes as disparidades observadas entre os países no tocante ao uso destas tecnologias, e grupos hegemônicos já se caracterizam em diferentes nichos com elevada dinamicidade - apenas para citar-se um exemplo, a língua inglesa já deixa de ser a mais utilizada na internet, e temas como a inclusão digital, a melhora e a disseminação de serviços públicos e a universalização daquelas tecnologias, com seu uso adequado pelo maior número de pessoas assumem papel cada vez mais preponderante, determinando os traços de uma nova geopolítica, a qual deve ser, necessariamente, contemplada quando da definição de estratégias destinadas aos cidadãos - não somente os atingidos pela cidadania digital -, e aos usuários de sistemas de informação, que não mais se encontram isolados em seus lares e salas de trabalho ou de estudo, mas sim conectados, virtualmente, ao mundo.

Exemplos de políticas ou de estudos sobre políticas encampando as preocupações com as tecnologias de informação e de comunicação surgem em todo o globo (MUIR; OPPENHEIM, 2002a, 2002b, 2002c, 2002d), citando-se especificamente os casos da União Européia (DAI, 2003), que se vê às voltas com o problema da desigualdade entre os seus países-membros e com a acomodação de diferentes culturas e línguas, tais como Itália (GARIBALDO, 2002), França (BARON; BRUILLARD, 2003; ROCHET, 2004) e Espanha (CORNELLA, 1998), além da Índia (ASHRAF, 2004), que apresenta diferenças gritantes entre os diferentes estratos da população também no que diz respeito ao acesso aos recursos da informação e, como não poderia deixar de ser, dos Estados Unidos, onde manifestam-se acentuadas desigualdades tecnológicas e culturais entre os diferentes estados da federação (GIL-GARCÍA, 2004).

No Brasil, já foram propostas políticas para a iniciativa do governo eletrônico (PINTO, 2001), e percebe-se a necessidade de iniciativas para formulação de políticas governamentais e organizacionais voltadas à informação (JOIA, 2004; MARCONDES; JARDIM, 2003; TELEFÔNICA, 2002). A ação governamental é (ou se propunha ser até a administração anterior) pautada por iniciativas como o “Livro Verde” (TAKAHASHI, 2000), originalmente destinado à inclusão digital e à formação de uma infra-estrutura nacional para a disseminação de informações e conteúdos digitais, e pelo “Livro Branco” (MCT, 2002), destinado à normatização das ações nacionais quanto à ciência, tecnologia e inovação (e que experimentou o mesmo processo de adoção e ostracismo que o Livro Verde), elementos que têm estreita associação com as políticas de desenvolvimento e competitividade industriais em mercados nacionais e globais (HALL; ANDRIANI, 2002).

7.4 Políticas de informação

Diversas abordagens têm sido propostas para a formulação de políticas de informação, desde a conceituação e a proposta de redefinição dos termos envolvidos (BROWNE, 1997a, 1997b; BRAMAN, 1989), dadas as peculiaridades da informação, tais como o fato de ser um "bem de experiência" (é necessário experimentá-la, ou seja, conhecê-la, para saber como ela é) e a elevada facilidade de sua reprodução (altos custos de produção, mas custos de reprodução baixos, por vezes ínfimos) (SHAPIRO, 1999, p. 36).

Com efeito, a Sociedade da Informação, antevista por Masuda (1982) e discutida em profundidade por autores como Castells (2003), Hardt e Negri (2001) e Browning, Halcli e Webster (2000), dentre muitos outros, requer alguns pré-requisitos para a sua efetivação. O próprio Masuda já estabelecia em sua obra que, qualquer que fosse a combinação obtida na implementação desta sociedade, a participação do cidadão é essencial (MASUDA, 1982, p. 104), motivada pela expansão do efeito multiplicador da produção da informação, pela tomada de decisões autônomas em grupo e por evitar-se a tendência a uma sociedade administrativamente centralizada. Tal sociedade está associada a uma economia em que a informação está no centro de suas necessidades econômicas, e na qual ambas, economia e sociedade, crescem e se desenvolvem em função da produção e do uso de valores informacionais, e onde a importância da informação como produto econômico excede a de bens, energia e serviços, modificando a própria estrutura da *urbe* e dos relacionamentos e serviços oferecidos no convívio urbano, como se pode ver, por exemplo, em Ishida e Isbister (2000) e em Castells (2003).

Embora seja comum supor-se que a Sociedade da Informação é uma sucessora radical da economia industrial, substituindo-a e com ela não convivendo (COSTA, 1999), tal fato não ocorre imperativamente: elas podem coexistir. Com efeito, estes dois estágios econômicos estão presentes ao mesmo tempo, numa economia composta, por todo o planeta (HARDT; NEGRI, 2001, p. 310). Além disso, durante o processo de produção voltado à informação, quando realizado coletivamente, constrói-se uma nova realidade, rumo a uma cidadania global. Esta nova cidadania cultua simultaneamente o eterno e o efêmero, num processo que alcança a seqüência passada e futura das expressões culturais dos indivíduos que a compõem, ao mesmo tempo em que depende do contexto e do objetivo do contexto cultural que é apresentado (CASTELLS, 2003, p. 487). Neste contexto, considera-se cultura como o complexo que inclui crenças, habilidades, artes, moral, costumes e aptidões físicas ou intelectuais adquiridas pela convivência em sociedade, à maneira de McGarry (1999, p. 62).

Do ponto de vista estratégico ou governamental, a Sociedade da Informação comporta três

tendências inter-relacionadas, a saber (MIRANDA, 2003, p. 60):

1. Integração vertical, estimulada pela desregulação e competição, num mercado mundial crescente, e onde inserem-se tendências como o software livre e a cessão coletiva de direitos autorais;
2. Globalização do mercado da produção intelectual, com produtos de caráter crescentemente internacional;
3. Privatização, caracterizada pela predominância de interesses privados - por vezes, em detrimento do interesse público -, controlando as empresas e, em particular, as organizações da área de comunicações e de informação.

Tendo em vista este cenário, devem-se implementar mecanismos que assegurem a devida inserção dos cidadãos no contexto desta Sociedade. Nos países em desenvolvimento, tais como a Índia (ASHRAF, 2004) e o Brasil (FGV, 2003), dentre outros, este é um desafio que se mostra ainda mais vultoso à luz de grandes deficiências e problemas que, historicamente, se avolumaram rumo à situação hoje vivenciada, que se contrapõe à inclusão digital.

É fato sabido que a informação tem papel essencial na elaboração, implementação e avaliação de políticas públicas (FERREIRA, 2003), quaisquer que sejam estas; o que dizer, então, quanto estas políticas têm por objetivo justamente a informação? A coleta, armazenamento, disseminação, tratamento e descarte da informação de modo adequado, realçando-a como um bem de valor impreditível, por sua fluidez e dependência intrínseca do contexto em que se insere, é fundamental para os países e organizações que desejam se introduzir ou se diferenciar no contexto informacional vigente. Neste sentido, a formulação de políticas voltadas à pesquisa e ao desenvolvimento de tecnologias baseadas no uso dos acervos e tecnologias de informação existentes assume elevado destaque, como se vê em Tassey (2004).

De todo este apanhado, obtém-se a seguinte definição:

Definição 7.2 *Uma* ***política de informação*** *é uma* política *voltada à caracterização, ao delineamento e à definição de ações voltadas à utilização da informação como ativo transformador da sociedade nas esferas governamentais, organizacionais e privadas.*

7.4.1 Fontes das políticas de informação

A busca, bastante acentuada após a Segunda Guerra Mundial, por maiores e melhores fontes e formas de acesso à informação tem se acelerado nos últimos anos. O advento da internet

potencializou ainda mais os conceitos de produção e disseminação rápidas da informação. Naturalmente, a qualidade da informação produzida e disseminada não acompanha de modo *pari passu* o volume informacional tornado disponível pelas diferentes origens. Do mesmo modo, a informação não é igualmente produzida de maneira uniforme por todos os países, organizações e grupos sociais. Como em qualquer outra atividade, existem *loci* de produção e consumo acentuados de determinados conteúdos, gerando uma elite e uma periferia informacionais cuja distância tende a se agravar, caso não sejam tomadas medidas capazes de aproximar os usuários da periferia dos meios e recursos de que necessitam para a produção e o intercâmbio de informações. Neste contexto, as políticas públicas da informação, mormente em países em desenvolvimento, assumem papel preponderante quanto à inclusão dos cidadãos como usuários e provedores habilitados das novas mídias - a informação assume um caráter de recurso nacional de altíssimo valor.

Embora o papel da informação no desenvolvimento sócio-econômico de uma sociedade ainda não esteja perfeitamente claro, e mesmo não sendo perfeitamente conhecidos quais os mecanismos essenciais à formação de uma sociedade da informação (uma vez que em diferentes contextos nacionais aplicam-se modalidades e graus diferentes de atuação pública), algumas características são observadas como pontos em comum em diferentes países pelo globo (ARNOLD, 2004, com adaptações) :

1. a informação é publicada e distribuída como um produto econômico, sendo colocada à disposição da sociedade em diferentes formatos e por diferentes canais;

2. a informação desempenha papel essencial como um recurso de caráter nacional, e, se administrada corretamente, pode impulsionar de modo substancial o desenvolvimento de uma nação. Para tanto, ela deve estar acessível e disponível a todos os segmentos - industrial, educacional, de lazer e entretenimento, econômico e político;

3. o valor da informação ou do conhecimento que se pode obter ou produzir por meio dela não é preditível, e, em decorrência disso, pode se modificar ao longo do tempo, aumentando ou diminuindo conforme a sua utilização - a gestão, a proteção e a valoração da informação não podem ser feitos como outros bens de produção ou de consumo;

4. os governos e órgãos públicos devem desenvolver e aplicar políticas voltadas à pesquisa e ao desenvolvimento das tecnologias da informação;

5. o acesso e a disponibilidade da informação tendem a estar associados ao desenvolvimento sócio-econômico - os cidadãos de países onde a sociedade da informação se apresenta de

modo acentuado possuem acesso a maiores volumes de informação de melhor qualidade, devido, em parte, à melhor infra-estrutura e a sistemas de telecomunicações mais desenvolvidos; por outro lado, este acesso gera a demanda por melhores meios e canais, o que realimenta o ciclo de acesso e disponibilidade de informação.

Devido às discrepâncias entre as diferentes realidades nacionais, cada país se lança de modo próprio na formulação de uma política nacional da informação, contemplando os aspectos nacionais e internacionais relevantes ao seu contexto em particular. Este desenvolvimento de políticas tem sua origem associada e voltada aos seguintes fatores, adaptados de Arnold (2004):

1. existe um movimento irrefutável, de âmbito global, em direção ao incremento da economia voltada à informação, em detrimento da produção industrial e de outros tipos de serviços;
2. a informação tem se valorizado e se disseminado cada vez mais como uma *commodity*: ela pode ser, e é, produzida e distribuída em bases comerciais;
3. o desenvolvimento dos mercados da informação e de suas tecnologias e as aplicações decorrentes vêm movendo a economia mundial em direção a uma era pós-industrial, a chamada “era da informação”, caracterizada pela informação como força motriz da economia;
4. cada vez mais, a informação é percebida como um bem de valor econômico por suas aplicações na cadeia produtiva de variados bens e produtos;
5. a informação é essencial para o planejamento macro-econômico;
6. as tecnologias da informação vêm sendo cada vez mais utilizadas para distribuir a informação, num ciclo que influencia e potencializa a sua disponibilidade;
7. o alto custo de determinadas fontes de informação torna o seu acesso restrito, ou mesmo impraticável; nestes casos, mesmo a presença dos recursos tecnológicos não é capaz de potencializar a disponibilidade de tais fontes, que devem ser então objeto de controles e gerenciamento (ou seja, políticas) particulares;
8. a publicação da informação por meios eletrônicos gera impacto na geração, distribuição e disponibilidade da informação relacionada, o que por sua vez influencia os mercados e o público consumidor - veja-se o exemplo do aumento acentuado da publicação eletrônica de artigos e periódicos científicos.

Conforme já foi dito, as políticas nacionais de informação sofrem influências dos contextos interno e externo para a sua efetivação. Dentre as influências nacionais, podem-se citar as seguintes (ARNOLD, 2004, com adaptações):

1. a abordagem e a variedade de termos e conceitos utilizados na política deve atender à realidade e à cultura nacionais;
2. as políticas são desenvolvidas de acordo com o valor que o governo e as entidades associadas atribuem à informação;
3. diferentes governos possuem diferentes motivos para desenvolver políticas de informação, dentre os quais salientam-se: orientar o setor de informações do país, proporcionar ou assegurar cooperações internas e externas, assegurar a disponibilidade e o acesso à informação e atender aos graus distintos de desenvolvimento, os quais apresentam necessidades distintas de acesso e uso da informação, além do fato de a realidade macroeconômica do país ditar a velocidade e a modalidade da implementação de infra-estrutura e de fontes de informação;
4. a política nacional pode ser única ou composta por várias políticas que se destinam a diferentes aspectos da economia da informação.

Dentre as influências externas, podem-se citar as seguintes, adaptadas de Arnold (2004):

1. a globalização e a competitividade requerem cada vez mais e melhores fontes e tecnologias de informação;
2. a informação tem importância cada vez maior como *commodity* negociável em mercados globais;
3. a propriedade e os direitos autorais sobre a informação e seus recursos tornam-se cada vez mais objeto de disputas legais;
4. a tecnologia e a infra-estrutura da informação apresentam crescimento mundial;
5. a mídia, como geradora e provedora de informação, tem papel crescente sobre as sociedades;
6. o acesso à informação é reconhecido como um direito inerente ao ser humano;
7. existe uma tendência mundial em direção ao desenvolvimento de políticas nacionais de informação.

7.4.2 Finalidades das políticas de informação

Além do campo de cobertura discutido acima, deve-se ter em mente, quando da formulação de uma política de informação, que ela deve atender a alguns princípios fundamentais, dentre os quais a estrita aderência à legislação, a promoção do intercâmbio de informações e mesmo a gestão da informação em agências e órgãos governamentais (CORNELLA, 1998). Deve-se evitar ainda a confusão comum entre educação tecnológica e educação para a informação: o fato de possuir-se recursos tecnológicos de uso disseminado não significa que o acesso e o uso da informação se darão de modo adequado - é preciso associar-se outras políticas de cunho social e educacional às iniciativas voltadas à informação.

Além do caráter sócio-econômico, as políticas podem ter ainda aspecto de orientação quanto à disseminação de informações de caráter público, por exemplo, quando da ocorrência de emergências ou calamidades nacionais (MAXWELL, 2003; QUINN, 2003). Outro aspecto relevante destas políticas se manifesta quando da formulação de programas de governo centrados nos cidadãos (SHULER, 2003), como para a formulação de estratégias G2C (*government to citizen*).

7.5 Princípios para as políticas de segurança da informação

A correta gestão da segurança da informação é atingida com o compromisso de todos os usuários quanto à aplicação das normas e procedimentos estabelecidos visando à padronização das ações de planejamento, implementação e avaliação das atividades voltadas à segurança (WILLIAMS, 2001). Estas diferentes atividades podem ser agrupadas conforme a seguinte disposição (ISACF, 2001):

1. Desenvolvimento de políticas, com os objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas;

2. Papéis e autoridades, assegurando que cada responsabilidade seja claramente entendida por todos;

3. Delineamento, desenvolvendo um modelo que consista em padrões, medidas, práticas e procedimentos;

4. Implementação, em um tempo hábil e com capacidade de manutenção;

5. Monitoramento, com o estabelecimento de medidas capazes de detectar e garantir correções às falhas de segurança, com a pronta identificação e atuação sobre falhas reais e suspeitas com plena aderência à política, aos padrões e às práticas aceitáveis;

6. Vigilância, treinamento e educação relativos à proteção, operação e prática das medidas voltadas à segurança.

Convém lembrar os princípios que a OCDE apresenta para o desenvolvimento de uma cultura de segurança da informação (OCDE, 2002b), já mostrados na Seção 5.8.4, e apenas resumidos aqui:

1. Vigilância;
2. Responsabilidade;
3. Participação;
4. Ética;
5. Democracia;
6. Avaliação de risco;
7. Delineamento e implementação da segurança;
8. Gestão da segurança;
9. Reavaliação.

Observa-se que o cumprimento de tais princípios é uma atividade discricionária, ou seja, cabe aos gestores decidir se aderem ou não às recomendações apresentadas. Pragmaticamente, cada vez mais empresas buscam a aderência a padrões internacionais ou nacionais de segurança, mesmo que advindos de fóruns externos. No espectro governamental, há algumas imposições. Cabe menção especial à disposição da Constituição brasileira, que estabelece que

> A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência (...) (BRASIL, 2004, Art. 37)

Embora estes princípios sejam comumente vistos como aplicáveis somente aos procedimentos e aos trâmites ligados às atividades da administração, como a gestão de pessoal e de finanças, não há nada que impeça a sua aplicação à segurança da informação. Ao contrário, como os procedimentos e trâmites da administração têm cada vez mais apoio sobre os sistemas de informação, a aplicação dos princípios dispostos pela Carta Magna a estes sistemas vem ao

encontro da intenção do constituinte: garante-se que os sistemas de informação sejam aderentes aos princípios legais vigentes, de ampla utilização, atentem para os preceitos da moral e da ética, dêem vazão aos anseios democráticos por acesso à informação e atendam eficientemente aos objetivos e requisitos para os quais foram criados.

Esta discussão orientou a formulação da seguinte definição:

Definição 7.3 *Uma **política de segurança da informação** é um conjunto de regras, normas e procedimentos que regulam como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo estado, além dos recursos e usuários que com ela interagem. Todo o ciclo de vida da informação deve ser objeto da política.*

7.6 A proposta de um modelo para a construção de políticas de segurança da informação

Epistêmica e ontologicamente, existem diferentes abordagens à análise das políticas, enquanto objetos de estudo pertencentes ao domínio das ciências sociais. É corrente a acepção de que é virtualmente impossível classificá-las objetivamente, sendo as mesmas políticas classificadas diferentemente por pesquisadores distintos - políticas são conceitos, e não qualidades empiricamente mensuráveis (SMITH, 2002). Uma das abordagens propostas, a de Dixon e Dogan (2004), apresenta o campo ontológico como sendo dividido entre o estruturalismo, com as ações sociais causadas pelas estruturas sociais, e o conceito de agência, pelo qual as ações sociais têm sua gênese nas ações individuais. No campo epistemológico, os autores dividem a análise entre os campos do naturalismo, segundo o qual a realidade social é objetiva e material, e a hermenêutica, pela qual a realidade social é subjetiva e ideacional. Esta taxonomia tem sido aplicada por seus autores a diversos contextos, como a governança corporativa (DIXON; DOGAN, 2003b), a governança global (DIXON; DOGAN, 2003a) e as práticas de gestão e administração (DIXON; DOGAN, 2003c).

Do ponto de vista prático, assiste-se atualmente à adoção de diferentes modelos para a confecção de políticas de informação, com exemplos de extremos merecedores de destaque o caso coreano, onde o aparato do estado determina as diretrizes a serem seguidas, por vezes à revelia do mercado (FACKLER, 2006), e o caso norte-americano, onde, conforme já se disse, os modelos de políticas são fortemente influenciados pelas corporações (ELKIN-KOREN, 2001).

Além da questão fundamental acerca das políticas serem determinadas pelo estado ou pelo mercado face a uma regulação competitiva, ou uma mescla contando com a participação de am-

bos, como tem sido a tônica no caso da União Européia (DAI, 2003), a análise da dependência do caminho se interpõe uma vez mais: deve-se fazer uso das instituições disponíveis como facilitadoras da coordenação e da comunicação essenciais ao processo das políticas, em uma ação evolucionária, ou deve-se promover a quebra dos padrões vigentes, implementando-se novos procedimentos e buscando-se a formação ou a afluência de novas redes, em uma abordagem revolucionária?

Também para esta questão existe uma solução intermediária, o que, no caso brasileiro, pode ser visto neste exato momento, no tocante à discussão acerca do padrão de televisão digital a ser adotado no país. Enquanto já se aventava a possibilidade da escolha do padrão japonês pelo governo, teve início no Congresso Nacional a tramitação de um projeto de lei acerca do SBTVD - Sistema Brasileiro de Televisão Digital - de orientação aberta ao mercado das operadoras de telecomunicações, favoráveis ao padrão europeu (PINHEIRO, 2006). Cumpre observar que até este momento ainda não se procedeu a uma discussão aprofundada e abrangente acerca dos conteúdos e dos modelos de negócios subjacentes à televisão digital no Brasil. Por outro lado, no que diz respeito às políticas para a segurança da informação, é marcante a presença do aparato estatal: a análise realizada junto à legislação disponível no país, localizada na Seção 5.8.5, mostra que grande parte das leis e demais dispositivos legais e administrativos disponíveis contempla apenas o aparato estatal, salvo nos aspectos penais e judiciais, estando ausentes normas com a chancela pública que tratem diretamente das organizações privadas - estas têm seguido, como já se observou, a padronização adotada em outros países, mormente nos Estados Unidos da América. A ausência de documentação acerca da efetividade das normas adotadas dificulta sobremaneira a análise da adequação dos instrumentos utilizados. A leitura atenta dos padrões e leis disponíveis mostra ser essencial a adoção de uma estratégia conjunta entre o estado e o mercado, onde o primeiro supre as falhas deste último, com sua presença e poder de coerção, enquanto este último alia sua maior agilidade e sua capacidade de investimentos e de produção às iniciativas do poder público.

A ênfase aos aspectos tecnológicos relativos à segurança da informação, já decantada neste trabalho, aliena da discussão acerca das normas e padrões um requisito fundamental a toda esta discussão: a questão da privacidade. De fato, em muitos casos, em prol da segurança corporativa ou nacional os usuários ou cidadãos têm se visto às voltas com o abandono da privacidade individual. Um modelo de políticas sociais para a segurança da informação deve ser capaz de equacionar estas variáveis, as quais, sabe-se, não têm sua convivência facilitada, gerando um quase paradoxo - como prover a segurança por meio de políticas públicas respeitando a privacidade individual (SHARPE; RUSSELL, 2003)?. Os trabalhos de Shapiro e Baker (2001), Levine (2003), Baker e Shapiro (2003) advogam que se faça uso de uma coalisão de esforços

envolvendo ações dos poderes judiciário e legislativo junto à iniciativa privada, de modo tal a garantir o correto funcionamento das instituições envolvidas. Uma vez mais, o Brasil tem exemplos recentes a mostrar em ambas as direções em um mesmo caso: enquanto o sigilo das informações pessoais é garantido constitucionalmente (BRASIL, 2004, Art. 5°, XII), sendo que sua quebra somente pode ocorrer em casos previstos em lei e sob autorização judicial (BRASIL, 1996), o caso recente envolvendo a quebra do sigilo bancário de um caseiro e o então ministro da Fazenda é emblemático no sentido de que muito ainda há para ser feito quanto à efetiva garantia das instituições legalmente dispostas. Contudo, isto não invalida o fato de que a **preservação da privacidade**, legalmente fundamentada e judicialmente respeitada, deve se sobrepor aos ditames da tecnologia e dos humores políticos ou mercadológicos. A construção da adequada atitude política, qual seja, a de respeito aos preceitos democráticos e legais, deve embasar a formulação das políticas acerca da privacidade individual, sobre a qual se alicerça a segurança da informação, nos ambientes corporativos e públicos.

Com este propósito, segue-se uma sugestão de um modelo para a elaboração de políticas de segurança da informação, baseado nas discussões elencadas ao longo deste trabalho. Este modelo segue a chamada multimetodologia, conforme apresentada em Mingers e Brocklesby (1997), a qual é sugerida, entre outros fins, para a elaboração e análise de modelos de sistemas de informação (MINGERS, 2001a; DAVIES; MABIN; BALDERSTONE, 2005; LEWIS; KELEMEN, 2002), sendo associada a outros modelos multimetodológicos, como a de sistemas flexíveis de Checkland (TORLAK, 2001) e à Teoria Geral dos Sistemas de von Bertalanffy (GOERGIOU, 2000). A multimetodologia se caracteriza por empregar uma análise multidisciplinar aos problemas tratados, uma vez revelada a complexidade destes. A característica da complexidade, por sinal, é amplamente apresentada pelas políticas e particularmente pelas políticas de segurança da informação, dado seu caráter normativo e eminentemente multidisciplinar, como se tem demonstrado ao longo deste trabalho. Naturalmente, o modelo proposto não tem por objetivo esgotar o problema, mas apenas resumir as considerações que já foram dispostas.

Seguindo-se a proposição apresentada em Mingers (2003), são apresentados os pressupostos que orientam a elaboração deste modelo, sob o ponto de vista da ontologia, da epistemologia e da axiologia (aquilo a que se atribui valor ou que considera correto):

ontologia - reconhece-se a problemática da segurança da informação, qual seja, a existência de um problema multidisciplinar e complexo, cuja complexidade se ilustra tanto pelo vulto da utilização das informações no âmbito das organizações quanto pela explosão dos incidentes e vulnerabilidades a que estão sujeitas e que permeiam todo o seu ambiente;

epistemologia - enxerga-se a informação e seus usuários sob o ponto de vista da fenome-

nologia, ou seja, como elementos igualmente constituintes dos sistemas de informação. Nem a informação o é sem a presença do usuário, nem este pode se manifestar, frente ao sistema, sem o concurso da informação à qual tem acesso;

axiologia - o elemento de valoração é a informação necessária aos sistemas: aquela que os usuários buscam ao realizarem seu acesso aos sistemas e que é por eles provida, analisada com o propósito de descrever, implementar e garantir a segurança da informação de modo tal a preservar a privacidade e os requisitos exigidos pela organização (vide Seção 4.4).

A Figura 10 ilustra a estratificação sugerida para a formulação das políticas de segurança da informação.

Figura 10: Um modelo para políticas de segurança da informação.

É conveniente salientar em que medida o modelo proposto atende aos objetivos deste trabalho, especificamente quanto à caracterização da segurança da informação como atinente ao domínio das ciências sociais. Neste sentido, antes de tudo deve-se lembrar que os sistemas de informação têm sua gênese nas necessidades apresentadas pelos usuários quanto às diferentes etapas do ciclo da informação, as quais, por sua vez, levam à formação das interações entre os mesmos usuários e destes com os sistemas. Em outras palavras, os sistemas de informação

devem atender a etapas muito bem definidas do *ethos* social - comunicar-se é uma atividade social, e os sistemas de informação estão voltados a propósitos eminentemente comunicacionais, interna ou externamente aos ambientes organizacionais.

Por sua vez, o perfeito entendimento das especificidades advindas destas interações, tais como o surgimento de ameaças e vulnerabilidades, deve estar intrinsecamente associado à formulação dos sistemas de informação, uma vez que ameaças e vulnerabilidades são, como se demonstrou, intrínsecas à própria construção de sistemas informacionais, e não somente os desenvolvidos com base computacional. A observação de comportamentos, tanto os inatos como os gerados pelo uso dos sistemas, bem como das necessidades dos usuários assume, assim, extrema relevância para o complexo da segurança da informação: somam-se oportunidades não vislumbradas em outros contextos a uma gama elevadíssima de formas de acesso e disponibilização de acervos informacionais.

Iniciando-se pelo reconhecimento do problema em seu contexto adequado, qual seja, derivado da construção social das interações que exigem a troca de informações e por conseguinte dão origem aos sistemas de informação, passa-se pela devida apreciação do papel do usuário e da informação no complexo da segurança: ao mesmo tempo em que a informação caracteriza o usuário, indicando sua interação com o sistema, o usuário cria, transforma e utiliza a informação. O contexto hermenêutico explora esta interação, ao interpretar as suas facetas salientes pela análise dos documentos que a determinam. Deste modo, as políticas são um produto da interação entre os usuários e seus pares, contemplando as redes e as forças presentes no momento de sua formulação e atentas às modificações aí apresentadas. O último nível é representado pelos programas, unidades administrativas das políticas, ou seja, o modo pelo qual elas são implementadas e acompanhadas. Diversas modalidades de formulação e acompanhamento de programas estão disponíveis, tais como o planejamento estratégico (PMI, 2000) ou o planejamento estratégico situacional (MATUS, 1992), mas sua discussão foge ao escopo deste trabalho.

8 Conclusões

8.1 Uma revisão dos passos propostos

Conforme apresentados na Seção 2.1, este trabalho se propôs a executar os seguintes passos, orientados pelas etapas metodológicas descritas na Seção 2.2:

1) realizar um amplo levantamento acerca do problema da segurança da informação e de como ele é tratado nos ambientes organizacionais e no ambiente governamental. Neste sentido, foram lidos mais de 1.400 textos, entre livros, artigos, modelos de políticas, relatórios e conteúdos de *sites* disponíveis na internet. Considera-se que a varredura realizada é abrangente e aprofundada o suficiente para embasar o trabalho apresentado;

2) fazer uso dos princípios da fenomenologia e da hermenêutica para a descrição de tal problema; o autor procurou realizar uma análise imparcial dos textos e documentos obtidos, isentando-se de pré-julgamentos que poderiam conspurcar esta análise;

3) caracterizar e tipificar as políticas de segurança da informação, apontando as suas origens e os passos para a sua formulação e implementação; foi feita uma coleta das principais fontes de fundamentação das políticas de segurança da informação no globo, com ênfase nos padrões internacionais;

4) apontar estratégias alternativas para a elaboração de tais políticas, visando a uma abordagem que se contraponha à usual, tecnicista, complementando-a com aspectos baseados na experiência do usuário frente aos sistemas de informação; a busca por esta abordagem alternativa consistiu na elaboração de um arcabouço baseado em disciplinas das ciências sociais, a fim de garantir uma abordagem efetivamente voltada ao usuário, culminando com um modelo baseado em requisitos ontológicos e epistemológicos para esta realização;

5) apontar complementos e acréscimos à abordagem escolhida para o problema. Estes complementos estão dispostos na seção 8.3, mais adiante.

8.2 Contribuições deste estudo para o estado da arte

Observando-se que a tecnologia da informação é adotada cada vez mais como uma tecnologia de representação do mundo, real ou virtual, gerando visões próprias da realidade objetiva, chega-se à observação de que a tecnologia aponta novos caminhos antes não concebidos. Assim sendo, o próprio uso da tecnologia por seus usuários constitui-se em um campo aberto a diversos questionamentos e considerações. No presente trabalho, por questões de escopo e praticidade, delimitou-se o campo de utilização das tecnologias da informação aos ambientes organizacionais nas esferas pública e privada, circunscritos aos sistemas de informação formais, ou seja, de utilização reconhecida na organização e utilizados com vistas aos fins organizacionais.

Este corte, longe de restringir o campo de pesquisa, permitiu o delineamento de uma ampla comparação com outros estudos. Diversos trabalhos foram analisados ao longo da confecção deste agora apresentado. No que diz respeito às políticas de segurança da informação, a imensa maioria privilegia os seus aspectos tecnológicos. Alguns citam a importância da observação ao usuário, mas poucos tratam em profundidade a sua problematização, em moldes tais como a utilização de um modelo para a apresentação das interações entre os usuários e deste com os sistemas, conforme sugerida por este trabalho. Desconhece-se ainda a existência de outros trabalhos que apresentam a segurança da informação como um domínio multidisciplinar das ciências sociais, apresentando sugestões de posturas epistemológicas para a sua abordagem.

Outra contribuição diz respeito ao delineamento da relação entre a abordagem fenomenológica e a Ciência da Informação, em busca de fundamentos epistemológicos que permitam a esta última tratar com seus objetos de estudo em bases filosoficamente fundamentadas.

Uma outra contribuição diz respeito à varredura do campo das políticas da segurança da informação do ponto de vista do contexto social - os estudos acerca destas políticas tratam-nas com base em aspectos tecnológicos. A abordagem adotada neste trabalho, procurando partir desde a nomenclatura e os conceitos envolvidos na formação de políticas de caráter geral, tenta elucidar este campo com vistas a uma correta formulação destes dispositivos.

8.3 Sugestões para estudos futuros

Várias outras disciplinas foram estudadas e diversas estratégias foram elaboradas ao longo da confecção deste trabalho, mas por problemas de ordem cronológica ou administrativa não foram levados a termo. Eis alguns destes estudos e estratégias:

1. a utilização de instrumentos (via de regra, questionários ou entrevistas) para a captação de percepções dos usuários de sistemas de informação quanto à sua segurança; estes instrumentos têm o intuito de reduzir a aversão normalmente causada pela implementação das políticas de segurança da informação e de contemplar questões pertinentes à compreensão das relações sociais no âmbito organizacional, propondo-se a análise do comportamento dos usuários frente à segurança da informação. Idealmente esta análise se daria pela aplicação de instrumentos em momentos prévio e posterior à adoção de tais políticas. A psicologia, em suas vertentes social e comportamental, apresenta várias modalidades para a construção e consecução de tais instrumentos (vide Apêndices A e B).

2. a análise das relações de poder intra-organizações a fim de mensurar o poder da organização quanto à implementação de políticas de segurança da informação;

3. a formalização das políticas por meio de mecanismos da lógica modal; ao longo deste estudo, foram desenvolvidos três modelos de lógicas modais para o tratamento de cláusulas acerca da segurança da informação, implementando os conceitos modais de obrigatoriedade, conhecimento e temporalidade (vide Apêndice C);

4. a criação de modelos baseados na teoria dos jogos para a análise das estratégias de formulação e aplicação de políticas. A teoria dos jogos é uma das disciplinas utilizadas para analisar os processos de tomada de decisão. Ela leva em consideração a modalidade de cooperação (ou de antagonismo) entre os participantes da ação modelada, a qual é caracterizada como um jogo, além de dedicar especial atenção à informação de posse de cada um dos participantes sobre o jogo em andamento - por exemplo, se cada participante tem ou não conhecimento sobre as ações tomadas pelos demais participantes -, além de considerar eventuais pressões sociais exercidas pelas escolhas dos demais sobre a decisão de determinado indivíduo, ou o altruísmo ali envolvido. Por estas razões, a teoria dos jogos foi considerada para a modelagem dos processos dinâmicos que se desenvolvem quando da adoção de políticas de segurança da informação, chegando a ser escrito um texto específico para este fim, mas, por considerações de tempo e escopo, como esta adoção está necessariamente concentrada na implementação das políticas, e não se chegou a um cronograma aceitável para a implementação de alguma política em alguma organização, tal desenvolvimento foi deixado para um estudo posterior.

8.4 Comentários finais

Uma constatação patente ao longo deste trabalho é a de que a solução proposta a um problema pode passar a ser um novo problema à espera de uma análise acurada, eventualmente ainda maior que o problema original. Em outras palavras, o uso de soluções pré-formatadas para a formulação ou a adoção de políticas pode ser mais danosa que a ausência de políticas, uma vez que se incorre em investimentos muitas vezes vultosos e cujo retorno não tem, por vezes, uma garantia assegurada.

Outro aspecto que merece especial atenção é a urgente necessidade de uma discussão aprofundada dos preceitos subjacentes às políticas de segurança da informação adotadas no Brasil - em sua maioria, do lado estatal, são voltadas ao próprio aparato do estado, salvo no tocante aos aspectos penais e judiciais. Do lado corporativo, carece-se de uma discussão adequada da realidade nacional frente ao fenômeno da Sociedade da Informação e dos modelos que a sociedade brasileira pretende adotar frente a esta realidade.

Por fim, cabe o comentário de que não se conhece qualquer solução meramente tecnológica para problemas sociais. Sendo um conceito eminentemente social, a segurança da informação necessita de uma visão igualmente embasada em conceitos sociais para sua correta cobertura.

Referências Bibliográficas

ABADI, M.; BLANCHET, B. Analyzing security protocols with secrecy types and logic programs. *Journal of the Association for Computing Machinery*, v. 52, n. 1, p. 102–146, Jan. 2005.

ACCORSI, R.; BASIN, D.; VIGANÒ, L. Towards an awareness-based semantics for security protocol analysis. *Electronic Notes on Theorical Computer Sciences*, v. 55, n. 1, p. 1–20, Jan. 2003.

ADAMS, F. The informational turn in philosophy. *Minds and Machines*, v. 13, n. 4, p. 471–501, Nov. 2003.

AHN, G.-J.; HONG, S.-P.; SHINC, M. E. Reconstructing a formal security model. *Information and Software Technology*, v. 44, n. 11, p. 649–657, Aug. 2002.

ALBERTS, C. J.; DOROFEE, A. J. *Managing Information Security Risks*: the OCTAVE approach. Boston: Addison-Wesley, 2002.

ALBERTS, C. J.; DOROFEE, A. J. Security incident response: rethinking risk management. *International Congress Series*, v. 1268, p. 141–146, June 2004.

ALCOFF, L. M. (Ed.). *Epistemology*: the big questions. Malden, Massachusetts: Blackwell, 1998.

ALFARO, L. de; GODEFROID, P.; JAGADEESAN, R. Three-valued abstractions of games: uncertainty, but with precision. In: *Proceedings of* 19^{th} *IEEE Symposium on Logic in Computer Science*. Turku, Finland: IEEE, 2004. p. 170–179.

ALJAREH, S.; ROSSITER, N. A task-based security model to facilitate collaboration in trusted multi-agency networks. In: *Proceedings of the 2002 ACM Symposium on Applied Computing*. Madri: ACM, 2002. p. 744–749.

ALUR, R.; HENZINGER, T. A.; KUPFERMAN, O. Alternating-time temporal logic. In: *Proceedings of the* 38^{th} *Annual Symposium on Foundations of Computer Science*. Oakland, California: IEEE, 1997. p. 1–9.

ALVES, C.; MENDES, V. Corporate governance policy and company performance: the Portuguese case. *Corporate governance*, v. 12, n. 3, p. 290–301, July 2004.

ANDERSON, J. M. Why we need a new definition of information security. *Computers & Security*, v. 22, n. 4, p. 308–313, May 2003.

ANDERSON, R. Why cryptosystems fail. In: *Proceedings of the* 1^{st} *ACM Conference on Computer and Communications Security*. Fairfax, Virginia, United States: ACM, 1993. p. 215–227. Disponível em: <http://doi.acm.org/10.1145/168588.168615>. Acesso em: 2 ago. 2004.

ANDERSON, R. *Why information security is hard*: an economic perspective. Cambridge, 2001. Disponível em: <http://www.cl.cam.ac.uk/ftp/users/rja14/econ.pdf>. Acesso em: 2 abr. 2004.

ANDERSON, R. Cryptography and competition policy: issues with ‘trusted computing’. In: *Proceedings of the 22nd Annual Symposium on Principles of Distributed Computing*. Boston, Massachusetts: ACM, 2003. p. 3–10. Disponível em: <http://doi.acm.org/10.1145/872035.872036>. Acesso em: 2 ago. 2004.

ANTÓN, A. I.; EARP, J. B.; CARTER, R. A. Precluding incongruous behavior by aligning software requirements with security and privacy policies. *Information and Software Technology*, v. 45, n. 14, p. 967–977, Nov. 2003.

ARBAUGH, W. Security: technical, social and legal challenges. *Computer*, v. 35, n. 2, p. 109–111, Feb. 2002.

ARCE, I. The rise of the gadgets. *IEEE Security & Privacy*, v. 1, n. 5, p. 78–81, Sept./Oct. 2003.

ARCE, I. The weakest link revisited. *IEEE Security & Privacy*, v. 1, n. 2, p. 72–76, Mar./Apr. 2003.

ARKENBOUT, E.; DIJK, F. van; WIJCK, P. van. Copyright in the information society: scenario’s and strategies. *European Journal of Law and Economics*, v. 17, n. 2, p. 237–249, Mar. 2004.

ARNOLD, A.-M. Developing a national information policy: considerations for developing countries. *The International Information & Library Review*, v. 36, n. 3, p. 199–207, Sept. 2004.

ASHFORTH, B. E.; KREINER, G. E. Normalizing emotion in organizations: making the extraordinary seem ordinary. *Human Resource Management Review*, v. 12, n. 2, p. 215–235, summer 2002.

ASHRAF, T. Information technology and public policy: a socio-human profile of Indian digital revolution. *The International Information & Library Review*, v. 36, n. 4, p. 309–318, Dec. 2004.

ASHRAFI, N. The impact of software process improvement on quality: in theory and practice. *Information & Management*, v. 40, n. 7, p. 677–690, Aug. 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 17799*: Tecnologia da informação - código de prática para a gestão da segurança da informação. Rio de Janeiro, 2002.

ATKINSON, M. M.; COLEMAN, W. D. Policy networks, policy communities and the problems of governance. *Governance*, v. 5, n. 2, p. 154–180, Apr. 1992.

AYOGU, M. D. Corporate governance in Africa: the record and policies for good corporate governance. *African Development Review*, v. 13, n. 2, p. 308–330, Dec. 2001.

BAERT, P. Pragmatism, realism and hermeneutics. *Foundations of science*, v. 8, n. 1, p. 89–106, Mar. 2003.

BAILLOT, P.; DANOS, V.; EHRHARD, T. Believe it or not, AJM's games model is a model of classical linear logic. In: *Proceedings of the* 12th *Annual IEEE Symposium on Logic in Computer Science*. Oakland, California: IEEE, 1997. p. 68–75.

BAKER, C. R.; SHAPIRO, B. Information technology and the social construction of information privacy: reply. *Journal of Accounting and Public Policy*, v. 22, n. 3, p. 287–290, May/June 2003.

BARBER, P. J.; LEGGE, D. *Percepção e Informação*. Rio de Janeiro: Zahar Editores, 1976.

BARON, G.-L.; BRUILLARD, E. Information and communication technology: models of evaluation in France. *Evaluation and Program Planning*, v. 26, n. 2, p. 177–184, Apr. 2003.

BASKERVILLE, R. Information systems security design methods: implications for informations systems development. *ACM Computing Surveys*, v. 25, n. 4, Nov. 1993.

BASS, F. T. Security policy: target, contents and links. In: *Proceedings of the* 21st *National Information Systems Security Conference*. NIST-National Institute of Standards and Technology, 1998. Disponível em: <http://csrc.nist.gov/nissc/1998/proceedings/paperG4.pdf>. Acesso em: 2 jun. 2003.

BATES, M. J. The invisible substrate of information science. *Journal of the American Society for Information Science*, v. 50, n. 12, 1999. Disponível em: <http://www.gseis.ucla.edu/faculty/bates/substrate.html>. Acesso em: 8 ago. 2003.

BAUMER, D. L.; EARP, J. B.; POINDEXTER, J. Internet privacy law: a comparison between the United States and the European Union. *Computers & Security*, v. 23, n. 5, p. 400–412, July 2004.

BEEBE, J. Can there be a science of the symbolic? *Journal of Analytical Psychology*, v. 49, n. 2, p. 177–191, May/June 2004.

BELLETTINI, C.; BERTINO, E.; FERRARI, E. Role based access control models. *Information Security Technical Report*, v. 6, n. 2, p. 21–29, June 2001.

BEN-ARI, M.; MANNA, Z.; PNUELI, A. The temporal logic of branching time. In: 8th *Annual ACM Symposium on Principles on Programming Languages*. New York: ACM, 1981. p. 164–176.

BIEBER, P.; CUPPENS, F. A logical view of secure dependencies. *Journal of Computer Security*, v. 1, n. 1, 1992. Disponível em: <http://www.rennes.enst-bretagne.fr/~fcuppens/articles/jcs92.ps>. Acesso em: 6 maio 2004.

BLATCHFORD, C. Information security, business and internet - part 1. *Network Security*, v. 2000, n. 1, p. 8–12, Feb. 2000.

BLATCHFORD, C. Information security, business and internet - part 2. *Network Security*, v. 2000, n. 2, p. 10–14, Mar. 2000.

BLOM-HANSEN, J. A 'new institutional' perspective on policy networks. *Public Administration*, v. 75, n. 4, p. 669–693, Jan. 1997.

BLOM-HANSEN, J. Policy-making in central-local government relations: balancing local autonomy, macroeconomic control, and sectoral policy goals. *Journal of Public Policy*, v. 19, n. 3, p. 237–264, Sept. 1999.

BOBBIO, N.; MATTEUCCI, N.; PASQUINO, G. *Dicionário de Política*. 4a. ed. Brasília: UnB, 1998.

BOEHM-DAVIS, D. A. Revisiting information systems as an interdisciplinary science. *Computers in Human Behavior*, v. 20, n. 2, p. 341–344, Mar. 2004.

BOLLOJU, N.; KHALIFA, M.; TURBAN, E. Integrating knowledge management into enterprise environments for the next generation decision support. *Decision Support Systems*, v. 33, n. 2, p. 163–176, June 2002.

BORKO, H. Information science: what is it? *American Documentation*, v. 19, n. 1, p. 3–5, Jan. 1968. Disponível em: <http://www-ec.njit.edu/ robertso/infosci/whatis.html>. Acesso em: 26 ago. 2003.

BÖRZEL, T. Organizing Babylon: on the different conceptions of policy networks. *Public Administration*, v. 76, n. 2, p. 252–273, Jan. 1998.

BOSSI, A. et al. Verifying persistent security properties. *Computer Languages, Systems & Structures*, v. 30, n. 3-4, p. 231–258, Oct./Dec. 2004.

BOSWORTH, S.; KABAY, M. E. (Eds.). *Computer Security Handbook*. 4th. ed. New York: John Wiley & Sons, 2002.

BRADLEY, S. (Ed.). *Governing the European Union*. New York: Sage Publications, 2001.

BRAGA, G. M. Informação, ciência da informação: breves reflexões em três tempos. *Ciência da Informação*, v. 24, n. 1, p. 84–88, Jan-Abr 1995.

BRAMAN, S. Defining information: an approach for policymakers. *Telecommunications Policy*, v. 13, n. 3, p. 233–242, Sept. 1989. Disponível em: <http://www.uwm.edu/∼braman/bramanpdfs/defining.pdf>. Acesso em: 16 nov. 2005.

BRASIL. *Código Penal*: Decreto-lei *n*° 2.840, de 7 de dezembro de 1.940. Brasília, 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Lei n° 8.159, de 8 de janeiro de 1.991*. Brasília, 1991. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8159.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Lei n° 9.296, de 24 de julho de 1.996*. Brasília, 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9296.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Lei n° 9.610, de 19 de fevereiro de 1.998*. Brasília, 1998. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9610.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Lei n° 9.883, de 7 de dezembro de 1999*. Brasília, 1999. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Decreto n° 3.505, de 13 de junho de 2.000*. Brasília, 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Decreto n° 3.587, de 5 de setembro de 2.000*. Brasília, 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/D3587.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Lei n° 9.983, de 14 de julho de 2.000*. Brasília, 2000. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L9983.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Decreto n° 3.872, de 18 de julho de 2.001*. Brasília, 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2001/D3872.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Decreto n° 3.996, de 31 de outubro de 2.001*. Brasília, 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2001/D3996.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Medida Provisória n° 2.200, de 24 de agosto de 2.001*. Brasília, 2001. Disponível em: <https://www.planalto.gov.br/ccivil_03/MPV/2200-2.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Código Civil*: Lei *n°* 10.406, de 10 de janeiro de 2.002. Brasília, 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Decreto n° 4.073, de 3 de janeiro de 2.002*. Brasília, 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4073.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Decreto n° 4.376, de 13 de setembro de 2.002*. Brasília, 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4376a.htm>. Acesso em: 10 jan. 2005.

BRASIL. *Decreto n° 4.553, de 27 de dezembro de 2.002*. Brasília, 2002. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/2002/D4553Compilado.htm>. Acesso em: 10 jan. 2005.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*. Brasília, 2004. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao.htm>. Acesso em: 10 jan. 2005.

BREWER, D. F. C.; NASH, M. J. The chinese wall security policy. In: *IEEE Symposium on Researh in Security and Privacy*. IEEE, 1989. Disponível em: <http://www.cs.purdue.edu/homes/cs590s/chinese-wall.pdf>. Acesso em: 19 fev. 2005.

BROWNE, M. The field of information policy: 1. Fundamental concepts. *Journal of Information Science*, v. 23, n. 4, p. 261–275, Aug. 1997.

BROWNE, M. The field of information policy: 2. Redefining the boundaries and methodologies. *Journal of Information Science*, v. 23, n. 5, p. 339–351, Oct. 1997.

BROWNING, G.; HALCLI, A.; WEBSTER, F. (Eds.). *Understanding Contemporary Society*: theories of the present. New York: Sage Publications, 2000.

BRUZINA, R. Phenomenology and cognitive science: moving beyond the paradigms. *Husserl Studies*, v. 20, n. 1, p. 43–88, Jan. 2004.

BUDD, J. M. Phenomenology and information studies. *Journal of Documentation*, v. 61, n. 1, p. 44–59, 2005.

BURKITT, I. Psychology in the field of being: Merleau-Ponty, Ontology and social constructionism. *Theory & Psychology*, v. 13, n. 3, p. 319–338, Jan. 2003.

BUSENBERG, G. J. Learning in organizations and public policy. *Journal of Public Policy*, v. 21, n. 2, p. 173–189, May 2001.

CAIRNS, D. Phenomenology and present-day psychology. *Phenomenology and the Cognitive Sciences*, v. 1, n. 1, p. 69–77, 2002.

CAMPBELL, K. et al. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, v. 11, n. 3, p. 431–448, 2003.

CAPURRO, R. *Heidegger y la experiencia del lenguaje*. 1982. Disponível em: <http://www.capurro.de/boss.htm>. Acesso em: 24 maio 2005.

CAPURRO, R. *Hermeneutics and the phenomenon of information*. 2000. Disponível em: <http://www.capurro.de/ny86.htm>. Acesso em: 24 maio 2005.

CARLSSON, L. Policy networks as collective action. *Policy Studies Journal*, v. 28, n. 3, p. 502–520, Aug. 2000.

CARR, R.; TYNAN, M.; DAVIS, R. Quality and security, they work together. *IEEE Aerospace and Electronic Systems Magazine*, v. 6, n. 9, p. 15–19, Sept. 1991.

CASTELLS, M. *A sociedade em rede*. 7. ed. São Paulo: Paz e Terra, 2003.

CAVALLI, E. et al. Information security concepts and practices: the case of a provincial multi-specialty hospital. *International Journal of Medical Informatics*, v. 73, n. 3, p. 297–303, Mar. 2004.

CHAUI, M. *Convite à Filosofia*. 12. ed. São Paulo: Ática, 1999.

CHOLVY, L.; CUPPENS, F. Analyzing consistency of security policies. In: 18th *IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE Computer Society, 1997. Disponível em: <citeseer.ist.psu.edu/article/laurence97analyzing.html>. Acesso em: 10 abr. 2004.

CHOU, S.-C. Dynamic adaptation to object state change in an information flow control model. *Information and Software Technology*, v. 46, n. 11, p. 729–737, Sept. 2004.

CHOU, S.-C. Providing flexible access control to an information flow control model. *The Journal of Systems and Software*, v. 73, n. 3, p. 425–439, Nov./Dec. 2004.

CHOU, S.-C. An agent-based inter-application information flow control model. *The Journal of Systems and Software*, v. 75, n. 1-2, p. 179–187, Feb. 2005.

CHRISTENSEN, J. G.; PALLESEN, T. The political benefits of corporatization and privatization. *Journal of Public Policy*, v. 21, n. 3, p. 283–309, June 2001.

CHURCHMAN, C. W. *Introdução à teoria dos sistemas*. Rio de Janeiro: Vozes, 1972.

CIBORRA, C. *Digital technologies and the duality of risk*. London, 2004. Disponível em: <http://issoc.is.lse.ac.uk/IDM/DualityOfRisk.pdf>. Acesso em: 18 maio 2005.

CIBORRA, C. U. Crisis and foundations: an inquiry into the nature and limits of models and methods in the information systems discipline. *Journal of Strategic Information Systems*, v. 7, n. 1, p. 5–16, Mar. 1998.

CLARK, D. How copyright became controversial. In: *Proceedings of the* 12^{th} *annual conference on Computers, freedom and privacy*. San Francisco, California: ACM, 2002. p. 1–10. Disponível em: <http://doi.acm.org/10.1145/543482.543499>. Acesso em: 2 ago. 2004.

CLARK, D. D.; WILSON, D. R. A comparison of commercial and military computer security policies. In: *Proceedings of the 1987 IEEE Symposium on Security and Privacy*. Oakland, California: IEEE, 1987. p. 184–194. Disponível em: <http://www.cs.rice.edu/∼dwallach/courses/comp527_f2004/ClarkWilson87.pdf>. Acesso em: 22 fev. 2005.

COHEN, J. E. DRM and privacy. *Communications of the ACM*, v. 46, n. 4, p. 47–49, Apr. 2003.

COLEMAN, J. Assessing information security risk in healthcare organizations of different scale. *International Congress Series*, v. 1268, p. 125–130, June 2004.

COLLMANN, J. et al. Beyond good practice: why HIPAA only addresses part of the data security problem. *International Congress Series*, v. 1268, p. 113–118, June 2004.

COMPUTER-BASED PATIENT RECORD INSTITUTE. *CPRI Toolkit*: Managing information security in health care. Schaumburg, IL, 2003. Disponível em: <http://www.himss.org/content/files/CPRIToolkit/version4/pdf/full_toolkit.pdf>. Acesso em: 17 fev. 2004.

COMPUTER EMERGENCY RESPONSE TEAM. *CERT/Coordination Center Statistics*. Pittsburgh, Carnegie Mellon University, Jan. 2004. Disponível em: <http://www.cert.org/stats/cert_stats.html>. Acesso em: 5 abr. 2004.

COMPUTER EMERGENCY RESPONSE TEAM. *Site oficial*. Pittsburgh, 2004. Disponível em: <www.cert.org>. Acesso em: 9 maio 2003.

COREN, S.; WARD, L. W. *Sensation and Perception*. Forth Worth: Harcourt Brace Jovanovich College Publishers, 1989.

CORNELIUS, I. Information and its philosophy. *Library Trends*, v. 52, n. 3, p. 377–386, Winter 2004.

CORNELLA, A. Information policies in Spain. *Government Information Quarterly*, v. 15, n. 2, p. 197–220, 1998.

COSTA, I. T. M. Informação, trabalho e tempo livre: políticas de informação para o século XXI. *Ciência da Informação*, v. 28, n. 2, p. 17–19, Maio/Ago. 1999.

CROTEAU, A.-M.; BERGERON, F. An information technology trilogy: business strategy, technological deployment and organizational performance. *Journal of Strategic Information Systems*, v. 10, n. 2, p. 77–99, June 2001.

CROWELL, S. G. Does the Husserl/Heidegger feud rest on a mistake? An essay on psychological and transcendental phenomenology. *Husserl Studies*, v. 18, n. 2, p. 123–140, Jan. 2002.

CUPPENS, F.; SAUREL, C. Specifying a security policy. In: *Proceedings of* 9^{th} *IEEE Workshop on Computer Security Foundations*. Kenmare, Kerry, Ireland: Kluwer Academic Publishers, 1996. p. 123–134. Disponível em: <http://www.rennes.enst-bretagne.fr/~fcuppens/articles/csfw96.ps>. Acesso em: 21 maio 2004.

DAI, X. A new mode of governance? Transnationalisation of european regions and cities in the information age. *Telematics and Informatics*, v. 20, n. 3, p. 193–213, Aug. 2003.

DAMIANOU, N. et al. The Ponder policy specification language. In: *Proceedings of the 2001 Workshop on Policies for Distributed Systems and Networks*. Bristol: Springer-Verlag, 2001. p. 19–39.

DAVIDOFF, L. L. *Introdução à Psicologia*. Rio de Janeiro: McGraw-Hill, 1983.

DAVIES, J.; MABIN, V.; BALDERSTONE, S. The theory of constraints: a methodology apart? - a comparison with selected OR/MS methodologies. *Omega*, v. 33, n. 6, p. 506–524, Dec. 2005.

DAVIES, W. Understanding strategy. *Strategy & Leadership*, v. 28, n. 5, p. 25–30, Oct. 2000.

DAVIS, M. S. Georg Simmel and Erving Goffman: legitimators of the sociological investigation of human experience. *Qualitative Sociology*, v. 20, n. 3, p. 369–388, Oct. 1997.

DAWSON, S.; QIAN, S.; SAMARATI, P. Providing security and interoperation of heterogeneous systems. *Distributed and Parallel Databases*, v. 8, n. 1, p. 119–145, Jan. 2000.

DEETZ, S. An understanding of science and a hermeneutic science of understanding. *The Journal of Communication*, v. 23, n. 2, p. 139–159, June 1973.

DESOUZA, K. C.; VANAPALLI, G. K. Securing knowledge in organizations: lessons from the defense and intelligence sectors. *International Journal of Information Management*, v. 25, n. 1, p. 85–98, Feb. 2005.

DHILLON, G. Dimensions of power and IS implementation. *Information & Management*, v. 41, n. 5, p. 635–644, May 2004.

DIAS, C. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel, 2000.

DICKHAUT, J. et al. Information management and valuation: an experimental investigation. *Games and Economic Behavior*, v. 44, n. 1, p. 26–53, July 2003.

DIXON, J.; DOGAN, R. Analyzing global governance failure: A philosophical framework. *Journal of Comparative Policy Analysis*, v. 5, n. 2-3, p. 209–226, June 2003.

DIXON, J.; DOGAN, R. Corporate decision making: contending perspectives and their governance implications. *Corporate Governance*, v. 3, n. 1, p. 39–57, 2003. Disponível em: <http://dx.doi.org/10.1108/14720700310459854>. Acesso em: 20 mar. 2006.

DIXON, J.; DOGAN, R. A philosophical analysis of management: improving praxis. *Journal of Management Development*, v. 22, n. 6, p. 458–482, 2003.

DIXON, J.; DOGAN, R. The conduct of policy analysis: Philosophical points of reference. *Review of Policy Research*, v. 21, n. 4, p. 559–579, July 2004.

DRAUCKER, C. B. The critique of heideggerian hermeneutical nursing research. *Journal of Advanced Nursing*, v. 30, n. 2, p. 360–373, Aug. 1999.

DREYFUS, H. L. The current relevance of Merleau-Ponty's phenomenology of embodiment. *Electronic Journal of Analytic Philosophy*, v. 4, 1996. Disponível em: <http://www.focusing.org/apm_papers/dreyfus2.html>. Acesso em: 19 abr. 2004.

DREYFUS, H. L. Why we do not have to worry about speaking the language of the computer. *Information Technology & People*, v. 11, n. 4, p. 281–289, 1998.

DUNN, P. The importance of consistency in establishing cognitive-based trust: a laboratory experiment. *Teaching Business Ethics*, v. 4, n. 3, p. 285–306, Aug. 2000.

E-COMMERCE.ORG. *Dados estatísticos sobre a internet e comércio eletrônico*. São Paulo, 2006. Disponível em: <http://www.e-commerce.org.br/STATS.htm>. Acesso em: 9 maio 2006.

ELKIN-KOREN, N. The privatization of information policy. *Ethics and Information Technology*, v. 2, n. 4, p. 201–209, Dec. 2001.

ELOFF, J.; ELOFF, M. Information security management: a new paradigm. In: *Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology*. Pretoria: South African Institute for Computer Scientists and Information Technologists, 2003. p. 130–136.

ELOFF, M. M.; VON SOLMS, S. H. Information security management: a hierarchical framework for various approaches. *Computers & Security*, v. 19, n. 3, p. 243–256, 2000.

ELSAS, P. I.; VRIES, P. M. O. de; RIET, R. P. van de. Computing conspiracies. In: *Proceedings of the 9th International Workshop on Database and Expert Systems Applications*. Viena: IEEE, 1998. p. 256–266.

EMBSE, T. J. von der; DESAI, M. S.; DESAI, S. How well are corporate ethics codes and policies applied in the trenches? Key factors and conditions. *Information Management & Computer Security*, v. 12, n. 2, p. 146–153, 2004.

EPSTEIN, R. L. *The semantic foundations of logic*: Propositional logic. London: Kluwer Academic Publishers, 1990.

EPSTEIN, R. L. *The semantic foundations of logic*: Predicate logic. Oxford: Oxford University Press, 1994.

ERNST & YOUNG LLP. *Global Information Security Survey 2003*. Washington, 2003. Disponível em: <http://www.ey.com/global/download.nsf/International/TSRS_-_Global_Information_Security_Survey_2003.pdf>. Acesso em: 27 jul. 2004.

ESCHER, M. C. Escher woodcarving. *Psychology 351 - Psychology of Perception*, 2002. Disponível em: <http://www.owlnet.rice.edu/~psyc351/Images/Escher.jpg>. Acesso em: 2 dez. 2003.

EULAU, H.; ROTHENBERG, L. Life space and social networks as political contexts. *Political Behavior*, v. 8, n. 2, p. 130–157, June 1986.

EUROPEAN COMMISSION. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - part 1*. Bruxelas, 1995. Disponível em: <http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce>. Acesso em: 2 dez. 2003.

EUROPEAN COMMISSION. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data - part 2*. Bruxelas, 1995. Disponível em: <http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce>. Acesso em: 2 dez. 2003.

EUROPEAN COMMISSION. *Network and Information Security*: proposal for a european policy approach. Bruxelas, 2001. Disponível em: <http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0298en01.pdf>. Acesso em: 30 jul. 2004.

EUROPEAN COMMISSION. *Towards a knowledge-based Europe*: the European Union and the information society. Bruxelas, 2002. Disponível em: <http://europa.eu.int/information_society/newsroom/documents>. Acesso em: 2 dez. 2002.

EUROPEAN COMMISSION. *Executive summary on Data protection - Citizens*. Bruxelas, 2003. Disponível em: <http://europa.eu.int/comm/public_opinion/archives/ebs>. Acesso em: 2 dez. 2003.

EUROPEAN COMMISSION. *Executive summary on Data protection - Companies*. Bruxelas, 2003. Disponível em: <http://europa.eu.int/comm/public_opinion/flash>. Acesso em: 2 dez. 2003.

EVERETT, J. Organizational research and the praxeology of Pierre Bourdieu. *Organizational Research Methods*, v. 5, n. 1, p. 56–80, Jan. 2002.

FACKLER, M. In Korea, bureaucrats lead the technology charge. *The New York Times*, 16 mar. 2006. Disponível em: <http://www.nytimes.com/2006/03/16/business/worldbusiness/16seoul.html>. Acesso em: 20 mar. 2006.

FARN, K.-J.; LIN, S.-K.; FUNG, A. R.-W. A study on information security management system evaluation: assets,threat and vulnerability. *Computer Standards & Interfaces*, v. 26, n. 6, p. 501–513, Oct. 2004.

FELDMAN, J.; MIYAMOTO, J.; LOFTUS, E. F. Are actions regretted more than inactions? *Organizational Behavior and Human Decision Processes*, v. 78, n. 3, p. 232–255, June 1999.

FERNÁNDEZ-MOLINA, J. C.; PEIS, E. The moral rights for authors in the age of digital information. *Journal of the American Society for Information Science and Technology*, v. 52, n. 2, p. 109–117, Jan. 2001.

FERREIRA, M. C. et al. Desenvolvimento de um instrumento brasileiro para avaliação da cultura organizacional. *Estudos de Psicologia*, v. 7, n. 2, p. 271–280, jul./dez. 2002.

FERREIRA, R. da S. A sociedade da informação no Brasil: um ensaio sobre os desafios do Estado. *Ciência da Informação*, v. 32, n. 1, p. 36–41, jan./abr. 2003.

FLORES, F. et al. Computer systems and the design of organizational interaction. *ACM Transactions on Office Information Systems*, v. 6, n. 2, p. 153–172, 1988. Disponível em: <http://doi.acm.org/10.1145/45941.45943>. Acesso em: 7 abr. 2004.

FLORIDI, L. Information ethics: on the philosophical foundation of computer ethics. *Ethics and Information Technology*, v. 1, n. 1, p. 37–56, 1999.

FLORIDI, L. On defining library and information science as applied philosophy of information. *Social Epistemology*, v. 16, n. 1, p. 37–49, Jan. 2002.

FLORIDI, L. What is the philosophy of information? *Metaphilosophy*, v. 33, n. 1-2, p. 123–145, Jan. 2002.

FLORIDI, L. Two approaches to the philosophy of information. *Minds and Machines*, v. 13, n. 4, p. 459–469, Nov. 2003.

FLORIDI, L. What is the philosophy of information? In: ____. *The Blackwell Guide to the Philosophy of Computing and Information*. Oxford: Blackwell, 2003. Disponível em: <http://www.wolfson.ox.ac.uk/∼floridi/blackwell/chapters/introduction.pdf>. Acesso em: 23 jun. 2005.

FLORIDI, L. LIS as applied philosophy of information: a reappraisal. *Library Trends*, v. 52, n. 3, p. 658–665, Winter 2004.

FLORIDI, L. Open problems on the philosophy of information. *Metaphilosophy*, v. 35, n. 4, p. 554–582, July 2004.

FOLEY, S. N. Building chinese walls in standard unix. *Computers & Security*, v. 16, n. 6, p. 551–563, 1997.

FOLTZ, C. B.; CRONAN, T. P.; JONES, T. W. Have you met your organization's computer usage policy? *Industrial Management & Data Systems*, v. 105, n. 2, p. 137–146, 2005.

FONTANA, G.; GERRARD, B. A post keynesian theory of decision making under uncertainty. *Journal of Economic Psychology*, v. 25, n. 5, p. 619–637, Oct. 2004.

FORD, W. Standardizing information technology security. *StandardView*, ACM, v. 2, n. 2, p. 64–71, 1994. Disponível em: <http://doi.acm.org/10.1145/202949.202951>. Acesso em: 2 ago. 2004.

FRAGATA, J. *A fenomenologia de Husserl como fundamento da filosofia*. Braga: Cruz-Braga, 1959.

FRASER, B. *RFC 2196 - Site Security Handbook*. 1997. Disponível em: <http://www.ietf.org/rfc/rfc2196.txt>. Acesso em: 14 maio 2003.

FULFORD, H.; DOHERTY, N. F. The application on information security policies in large UK-based organizations: an exploratory investigation. *Information Management & Computer Security*, v. 11, n. 3, p. 106–114, 2003.

FUMY, W. IT security standardisation. *Network Security*, v. 2004, n. 12, p. 6–11, Dec. 2004.

FUNDAÇÃO GETÚLIO VARGAS. *Mapa da Exclusão Digital*. Rio de Janeiro: Centro de Políticas Sociais - Fundação Getúlio Vargas, 2003.

FURNELL, S. M.; CHILIARCHAKI, P.; DOWLAND, P. S. Security analysers: administrator assistants or hacker helpers? *Information Management & Computer Security*, v. 9, n. 2, p. 93–101, 2001.

GADAMER, H.-G. The hermeneutic circle: the elevation of the historicity of understanding to the status of a hermeneutic principle. In: ALCOFF, L. M. (Ed.). *Epistemology*: the big questions. Malden, Massachusetts: Blackwell, 1998. p. 232–247.

GALLAGHER, S.; VARELA, F. Redrawing the map and resetting the time: Phenomenology and the cognitive sciences. In: CROWELL, S.; EMBREE, L.; JULIAN, S. J. (Eds.). *The reach of reflection*. Delray Beach, Florida: Center for Advanced Research in Phenomenology, 2001. Disponível em: <http://www2.canisius.edu/~gallagher/G&V01.pdf>. Acesso em: 18 dez. 2002.

GARG, A.; CURTIS, J.; HALPER, H. Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, v. 11, n. 2, p. 74–83, 2003.

GARIBALDO, F. Information and communication technologies, organisations and skills: Convergence and persistence. *AI & Society*, v. 16, n. 4, p. 305–331, Nov. 2002.

GAUNT, N. Installing an appropriate information security policy. *International Journal of Medical Informatics*, v. 49, n. 1, p. 131–134, Mar. 1998.

GEANELLOS, R. Exploring Ricoeur's hermeneutic theory of interpretation as a method of analysing research texts. *Nursing Inquiry*, v. 7, n. 2, p. 112–119, June 2000.

GEER JR, D.; HOO, K. S.; JAQUITH, A. Information security: why the future belongs to the quants. *IEEE Security & Privacy*, v. 1, n. 4, p. 24–32, July/Aug. 2003.

GENERAL ACCOUNTING OFFICE. *Information Security Management*: learning from leading organizations. Washington - General Accounting Office, 1998. Disponível em: <http://www.gao.gov/special.pubs/ai9868.pdf>. Acesso em: 05 abr. 2004.

GENGLER, B. Content protection for recordable media. *Computer Fraud & Security*, v. 2001, n. 2, p. 5–6, Feb. 2001.

GEORGE, V. *The experience of being as goal of human existence*: the Heideggerian approach. Washington: The Council for research in Values and Philosophy, 2000. (Cultural heritage and contemporary change. IIIB, South Asia, v. 2).

GERBER, M.; VON SOLMS, R.; OVERBEEK, P. Formalizing information security requirements. *Information Management & Computer Security*, v. 9, n. 1, p. 32–37, 2001.

GERSBACH, H. Size and distributional uncertainty, public information and the information paradox. *Social Choice and Welfare*, v. 17, n. 2, p. 241–246, Mar. 2000.

GIBBS, J. L. The Digital Millennium Copyright Act. *Ubiquity*, v. 1, n. 26, p. 1–4, 2000. Disponível em: <http://doi.acm.org/10.1145/348790.348792>. Acesso em: 2 ago. 2004.

GIL-GARCÍA, J. R. Information technology policies and standards: a comparative review of the states. *Journal of Government Information*, v. 30, n. 5-6, p. 548–60, Sept. 2004.

GILLILAND, S. W.; SCHEPERS, D. W. Why we do the things we do: a discussion and analysis of determinants of just treatment in layoff implementation decisions. *Human Resource Management Review*, v. 13, n. 1, p. 59–83, Sept. 2003.

GLASGOW, J.; MACEWEN, G.; PANANGADEN, P. A logic for reasoning about security. *ACM Transactions on Computer Systems*, v. 10, n. 3, p. 226–264, 1992.

GODFREY-SMITH, P. Environmental complexity and the evolution of cognition. In: STERNBERG, R.; KAUFMAN, J. (Eds.). *The evolution of intelligence*. Stanford, California: Lawrence Erlbaum Associates, 2001.

GOERGIOU, I. The ontological constitution of bounding-judging in the phenomenological epistemology of Von Bertalanffy's General System Theory. *Systemic Practice and Action Research*, v. 13, n. 3, p. 391–424, June 2000.

GOLDKUHL, G.; ÅGERFALK, P. J. Action within information systems: outline of a requirements engineering method. In: *Proceedings of* 4^{th} *International Workshop on Requirements Engineering*: Foundation for software quality. Pisa: University of Pisa, 1998. Disponível em: <http://www.ida.liu.se/∼gorgo/erp/GGPAk-REFSQ98.pdf>. Acesso em: 12 abr. 2004.

GOODMAN, J.; HECKERMAN, D.; ROUNDTHWAITE, R. Stopping spam. *Scientific American*, v. 292, n. 4, p. 24–31, Apr. 2005.

GORDON, L. A.; LOEB, M. P. The economics of information security investment. *ACM Transactions on Information and Systems Security*, v. 5, n. 4, p. 438–457, Nov. 2002.

GORDON, L. A.; LOEB, M. P. Return on information security investments: myths vs. realities. *Strategic finance*, v. 84, n. 5, p. 26–31, Nov. 2002.

GORDON, L. A.; LOEB, M. P.; LUCYSHYN, W. Sharing information on computer systems security: an economic analysis. *Journal of Accounting and Public Policy*, v. 22, n. 6, p. 461–485, Nov/Dec. 2003.

GORDON, L. A. et al. *2004 CSI/FBI Computer crime and security survey*. Washington, 2004. Disponível em: <http://www.gocsi.com/forms/fbi/pdf.jhtml>. Acesso em: 9 jun. 2004.

GORDON, L. A.; LOEB, M. P.; SOHAIL, T. A framework for using insurance for cyber-risk management. *Communications of the ACM*, v. 46, n. 3, p. 81–85, Mar. 2003.

GORDON, L. A.; RICHARDSON, R. The new economics of information security. *Information Week*, n. 982, p. 53–56, Mar. 2004.

GRAMBERGER, M. *Citizens as partners*: OECD handbook on information, consultation and public participation in policy-making. Paris: OECD, 2001.

GREENER, I. Agency, social theory and social policy. *Critical Social Policy*, v. 22, n. 4, p. 688–705, Nov. 2002.

GREENER, I. Theorising path-dependency: How does history come to matter in organisations? *Management Decision*, v. 40, n. 6, p. 614–619, 2002.

GREENER, I. The potential of path dependence in political studies. *Politics*, v. 25, n. 1, p. 62–72, Feb. 2005.

GUAN, B.-C. et al. Evaluation of information security related risks of an organization: the application of the multi-criteria decision-making method. In: *IEEE 37th Annual International Carnahan Conference on Security Technology*. Oakland, California: IEEE Society, 2003. p. 168–175.

GUEL, M. D. *A short primer for developing security policies*. Bethesda, Maryland, 2001. Disponível em: <http://www.sans.org/resources/policies/Policy_Primer.pdf>. Acesso em: 25 abr. 2002.

GUPTA, M. et al. Matching information security vulnerabilities to organizational security profiles: a genetic algorithm approach. *Decision Support Systems*, 2004. No prelo.

GUZMAN, I. R.; KAARST-BROWN, M. L. Organizational survival and alignment: insights into conflicting perspectives on the role of the IT professional. In: *Proceedings of the 2004 conference on Computer personnel research*. Tucson, Arizona: ACM, 2004. p. 30–34. Disponível em: <http://doi.acm.org/10.1145/982372.982379>. Acesso em: 2 ago. 2004.

HAGUETE, T. M. F. A interação simbólica. In: ____. *Metodologias qualitativas na sociologia*. 4. ed. Petrópolis: Vozes, 1995. p. 25–50.

HALL, R.; ANDRIANI, P. Managing knowledge for innovation. *Long Range Planning*, v. 35, n. 1, p. 29–48, Feb. 2002.

HAMMONDS, G. L. et al. Command center security - proving software correct. In: *Proceedings of the* 10^{th} *annual conference on Systems Integrity, Software Safety and Proccess Security*. Oakland, California: IEEE, 1995. p. 163–173.

HANSSON, J. Hermeneutics as a bridge between the modern and the postmodern in library and information science. *Journal of Documentation*, v. 61, n. 1, p. 102–113, 2005.

HARDT, M.; NEGRI, A. *Império*. São Paulo: Record, 2001.

HARRIS, R.; BROWNING, R. Global monitoring for environment and security: data policy considerations. *Space Policy*, v. 19, n. 4, p. 265–276, Nov. 2003.

HAWKINS, S. M.; YEN, D. C.; CHOU, D. C. Awareness and challenges of internet security. *Information Management & Computer Security*, v. 8, n. 3, p. 131–143, 2000.

HAWKINS, S. M.; YEN, D. C.; CHOU, D. C. Disaster recovery planning: a strategy for data security. *Information Management & Computer Security*, v. 8, n. 5, p. 222–229, 2000.

HEAP, S. H. et al. *The theory of choice*: a critical guide. Oxford: Blackwell, 1992.

HECLO, H. H. Policy analysis. *British Journal of Political Science*, v. 2, n. 1, p. 83–108, Jan. 1972.

HEIDEGGER, M. On the essence of truth. 1943. Disponível em: <http://foucault.info/links/related-heidegger/heidegger.essenceOfTruth.eng.html>. Acesso em: 26 maio 2005.

HEIDEGGER, M. *Being and Time*. Oxford: Basil Blackwell, 1985.

HEIDEGGER, M. *Ser e Tempo*. 3. ed. Petrópolis: Vozes, 1993. V. 2.

HEIDEGGER, M. *The basic problems of the phenomenology*. Bloomington: Indiana University, 1998.

HEIDEGGER, M. *Ser e Tempo*. 12. ed. Petrópolis: Vozes, 2002. V. 1.

HEINÄMAA, S. Merleau-Ponty's modification of phenomenology: cognition, passion and philosophy. *Synthese*, v. 118, n. 1, p. 49–69, Jan. 1999.

HELVEY, T. et al. Data security in life sciences research. *Drug Discovery Today: BIOSILICO*, v. 2, n. 3, p. 97–103, May 2004.

HENESSY, D. A.; BABCOCK, B. A. Information, flexibility and value added. *Information Economics and Policy*, v. 10, n. 4, p. 431–449, Dec. 1998.

HENNING, R. R. Security service level agreements: quantifiable security for the enterprise? In: *Proceedings of the 1999 workshop on new security paradigms*. Ontario: ACM, 2000. p. 54–60.

HITCHENS, A. A call for inter-governmental organizations policies on public access to information. *Government Information Quarterly*, v. 14, n. 2, p. 143–154, 1997.

HITCHINGS, J. Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers & Security*, v. 14, n. 5, p. 377–383, May 1995.

HJØRLAND, B. Library and information science: practice, theory, and philosophical basis. *Information Processing and Management*, v. 36, n. 3, p. 501–531, May 2000.

HJØRLAND, B. Arguments for philosophical realism in library and information science. *Library Trends*, v. 52, n. 3, p. 488–506, Winter 2004.

HJØRLAND, B. Comments on the articles and proposals for further work. *Journal of Documentation*, v. 61, n. 1, p. 156–163, 2005.

HJØRLAND, B. Empiricism, rationalism and positivism in library and information science. *Journal of Documentation*, v. 61, n. 1, p. 130–155, 2005.

HJØRLAND, B. Library and information science and the philosophy of science. *Journal of Documentation*, v. 61, n. 1, p. 5–10, 2005.

HÖNE, K.; ELOFF, J. Information security policy: what do international information security standards say? *Computers & Security*, v. 21, n. 5, p. 402–409, Oct. 2002.

HÖNE, K.; ELOFF, J. What makes an effective information security policy? *Network Security*, v. 2002, n. 6, p. 14–16, June 2002.

HORLICK-JONES, T.; SIME, J. Living on the border: knowledge, risk and transdisciplinarity. *Futures*, v. 36, n. 4, p. 441–456, May 2004.

HOWARD, J. D.; MEUNIER, P. Using a "common language" for computer security incident information. In: BOSWORTH, S.; KABAY, M. E. (Eds.). *Computer Security Handbook*. 4th. ed. New York: John Wiley & Sons, 2002. p. 3.1–3.22.

HUDSON, J. E-galitarianism: The information society and New Labour's repositioning of welfare. *Critical Social Policy*, v. 23, n. 2, p. 268–290, May 2003.

HUGHES, G. E.; CRESSWEL, M. J. *A companion to modal logic*. London: Methuen and Co, 1984.

HUGHES, G. E.; CRESSWEL, M. J. *A new introduction to modal logic*. London: Routledge, 1996.

HUSSERL, E. *The crisis of european sciences and transcendental phenomenology*: an introduction to phenomenological philosophy. Evanston, Illinois: Northwestern University Press, 1970.

HUSSERL, E. *Investigações lógicas*: Sexta investigação - elementos de uma elucidação fenomenológica do conhecimento. São Paulo: Nova Cultural, 1996.

IDSON, L. C.; LIBERMAN, N.; HIGGINS, E. T. Distinguishing gains from nonlosses and losses from nongains: A regulatory focus perspective on hedonic intensity. *Journal of Experimental Social Psychology*, v. 36, n. 3, p. 252–274, May 2002.

INFORMATION SYSTEMS AUDIT AND CONTROL FOUNDATION. *Information security governance*: guidance for boards of directors and executive management. Rolling Meadows, Illinois, 2001.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATíSTICA. *Pesquisa anual do comércio - 2003*. Rio de Janeiro, 2003. Disponível em: <http://www.ibge.gov.br/home/estatistica/economia/comercioeservico/pac/2003/default.shtm>. Acesso em: 9 maio 2006.

INTRONA, L. D. The (im)possibility of ethics in the information age. *Information and Organization*, v. 12, n. 2, p. 71–84, Apr. 2002.

ISHIDA, T.; ISBISTER, K. (Eds.). *Digital cities*: technologies, experiences, and future perspectives. Berlim: Springer, 2000.

IT GOVERNANCE INSTITUTE. *COBIT Control Objectives*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Executive Summary*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Framework*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Implementation Tool Set*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Management Guidelines*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT security baselines*. Chicago, 2004. Disponível em: <http://www.isaca.org>. Acesso em: 17 jan. 2005.

IT GOVERNANCE INSTITUTE. *IT control objectives for Sarbanes-Oxley*. Rolling Meadows, Illinois, 2004. Disponível em: <http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=13923>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *IT governance global status report*. Rolling Meadows, Illinois, 2004. Disponível em: <http://www.itgi.org>. Acesso em: 1 fev. 2006.

IT GOVERNANCE INSTITUTE. *COBIT*. Chicago, 2005. Disponível em: <http://www.isaca.org>. Acesso em: 17 jan. 2005.

JAEGER, P. T.; BERTOT, J. C.; MCCLURE, C. R. The impact of the USA Patriot Act on collection and analysis of personal information under the Foreign Intelligence Surveillance Act. *Government Information Quarterly*, v. 20, n. 3, p. 295–314, July 2003.

JAMES, J. Free software and the digital divide: opportunities and constraints for developing countries. *Journal of Information Science*, v. 29, n. 1, p. 25–33, Feb. 2003.

JANICAUD, D. Toward a minimalist phenomenology. *Research in Phenomenology*, v. 30, n. 1, p. 89–106, Sept. 2000.

JASANOFF, S. The political science of risk perception. *Reliability Engineering and System Safety*, v. 59, n. 1, p. 91–99, 1998.

JENSEN, C.; POTTS, C. Privacy policies as decision-making tools: an evaluation of online privacy notices. In: *Proceedings of the 2004 conference on Human factors in computing systems*. Vienna, Austria: ACM, 2004. p. 471–478. Disponível em: <http://doi.acm.org/10.1145/985692.985752>. Acesso em: 2 ago. 2004.

JOIA, L. A. Developing government-to-government enterprizes in Brasil: a heuristic model drawn from multiple case studies. *International Journal of Information Management*, v. 24, n. 2, Apr. 2004.

JONSSON, E. An integrated framework for security and dependability. In: *Proceedings of the 1998 workshop on New security paradigms*. Charlottesville, Virginia, United States: ACM, 1998. p. 22–29. Disponível em: <http://doi.acm.org/10.1145/310889.310903>. Acesso em: 2 ago. 2004.

KAGAL, L.; FININ, T.; PENG, Y. *A framework for distributed trust management*. 2001. Disponível em: <http://csce.uark.edu/∼hexmoor/AA01/cameraready/Kagal.ps>. Acesso em: 2 mar. 2004.

KAHNEMAN, D. A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, v. 58, n. 9, p. 697–720, Sept. 2003.

KAHNEMAN, D.; TVERSKY, A. The psychology of preferences. *Scientific American*, v. 246, n. 1, p. 136–142, Jan. 1982.

KAPLAN, M.; CUCITI, P. Telecommunications in Brazil: Restructuring and privatization. *Journal of Project Finance*, v. 4, n. 1, p. 7–27, Spring 1998.

KARABACAK, B.; SOGUKPINAR, I. ISRAM: information security risk analysis method. *Computers & Security*, v. 24, n. 2, p. 147–159, Mar. 2005.

KARLSSON, I.; CHRISTIANSON, S.-A. The phenomenology of traumatic experiences in police work. *Policing: An International Journal of Police Strategies & Management*, v. 26, n. 3, p. 419–438, Sept. 2003.

KAROLY, P. Mechanisms of self-regulation: a systems view. *Annual Review of Psychology*, v. 44, p. 23–52, 1993.

KAY, A. A critique of the use of path dependency in policy studies. *Public Administration*, v. 83, n. 3, p. 553–571, Aug. 2005.

KEAST, R. et al. Network structures: Working differently and changing expectations. *Public Administration Review*, v. 64, n. 3, p. 363–371, May/June 2004.

KIM, J. Phenomenology of digital-being. *Human Studies*, v. 24, n. 1/2, p. 87–111, Mar. 2001.

KING, G. Best security practices: an overview. In: *Proccedings of the 23rd National Information Systems Security Conference*. NIST-National Institute of Standards and Technology, 2000. Disponível em: <http://csrc.nist.gov/nissc/2000/proceedings/papers/022.pdf>. Acesso em: 18 jul. 2003.

KLEIN, H. K. Seeking the new and the critical in critical realism: déjà vu? *Information and organization*, v. 14, n. 2, p. 123–144, Apr. 2004.

KLEITER, G. D. et al. Do subjects understand base rates? *Organizational Behavior and Human decision processes*, v. 72, n. 1, p. 25–61, Oct. 1997.

KO, I. S. et al. Distribution of digital contents based on public key considering execution speed and security. *Information Sciences*, v. 174, n. 3-4, p. 237–250, Aug. 2005.

KOCHER, P. et al. Security as a new dimension in embedded system design. In: *Proceedings of the* 41st *annual conference on Design automation*. ACM, 2004. p. 753–760. Disponível em: <http://doi.acm.org/10.1145/996566.996771>. Acesso em: 2 ago. 2004.

KOKOLAKIS, S. A.; KIOUNTOUZIS, E. A. Achieving interoperability in a multiple-security policies environment. *Computers & Security*, v. 19, n. 3, p. 267–281, May 2000.

KONANA, P.; BALASUBRAMANIAN, S. The social economic psychological model of technology adoption and usage: an application to online investing. *Decision Support Systems*, v. 39, n. 3, p. 505–524, May 2005.

KORZYK SR, A. A forecasting model for internet security attacks. In: *Proceedings of the 21st National Information Systems Security Conference*. NIST-National Institute of Standards and Technology, 1998. Disponível em: <http://csrc.nist.gov/nissc/1998/proceedings/paperD5.pdf>. Acesso em: 9 jun. 2003.

KRAUSE, M.; TIPTON, H. F. *Information Security Management Handbook*. New York: CRC Press - Auerbach, 1999.

KREMER, S.; RASKIN, J.-F. A game-based verification of non-repudiation and fair exchange protocols. *Lecture Notes in Computer Science*, v. 2154, p. 551–767, Aug. 2001.

KREMER, S.; RASKIN, J.-F. Game analysis of abuse-free contract signing. In: *Proceedings of the 15th IEEE Computer Security Foundations Workshop*. Oakland, California: IEEE, 2002. p. 206–220.

KRUTZ, R. L.; VINES, R. D. *The CISSP Prep Guide*: Gold edition. New York: John Wiley & Sons, 2002.

KWAK, Y. H.; LAPLACE, K. S. Examining risk tolerance in project-driven organization. *Technovation*, v. 25, n. 6, p. 691–695, June 2005.

KWOK, S. et al. SDMI-based rights management systems. *Decision Support Systems*, v. 38, n. 1, p. 33–46, Oct. 2004.

LAMARCHE, F. Games semantics for full propositional logic. In: *Proceedings of the 10th Annual Symposium on Logic in Computer Science*. Oakland, California: IEEE, 1995. p. 467–476.

LAMBRINOUDAKIS, C. et al. Security requirements for e-government services: a methodological approach for developing a common PKI-based security policy. *Computer Communications*, v. 26, n. 16, p. 1873–1883, Oct. 2003.

LEE, A. S. Thinking about social theory and philosophy for information systems. In: MINGERS, J.; WILLCOCKS, L. (Eds.). *Social theory and philosophy for information systems*. Chichester, UK: John Willey & Sons, 2004. p. 1–26. Disponível em: <http://media.wiley.com/product_data/excerpt/71/04708511/0470851171-1.pdf>. Acesso em: 20 nov. 2004.

LEE, J.; LEE, Y. A holistic model of computer abuse within organizations. *Information Management & Computer Security*, v. 10, n. 2, p. 57–63, 2002.

LEGRIS, P.; INGHAM, J.; COLLERETTE, P. Why do people use information technology: a critical review of the technology acceptance model. *Information & Management*, v. 40, n. 3, p. 191–204, Jan. 2003.

LEIWO, J.; HEIKKURI, S. An analysis of ethics as foundation of information security in distributed systems. In: *Proceedings of the* 31*st* *Hawaii International Conference on System Sciences*. Oakland, California: IEEE Society, 1998. v. 6, p. 213–222.

LEONARDO, Z. Interpretation and the problem of domination: Paul Ricoeur's hermeneutics. *Studies in Philosophy and Education*, v. 22, n. 5, p. 329–350, Sep. 2003.

LESK, M. *The seven ages of information retrieval*. 1995. Disponível em: <http://lesk.com/mlesk/ages/ages.html>.

LEVINE, P. Information technology and the social construction of information privacy: comment. *Journal of Accounting and Public Policy*, v. 22, n. 3, p. 281–285, May/June 2003.

LEWIS, M. W.; KELEMEN, M. L. Multiparadigm inquiry: Exploring organizational pluralism and paradox. *Human Relations*, v. 55, n. 2, p. 251–275, Feb. 2002.

LIAW, H.-T. A secure electronic voting protocol for general elections. *Computers & Security*, v. 23, n. 2, p. 107–119, Mar. 2004.

LIEN, M.-C.; PROCTOR, R. W. Multiple spatial correspondence effects on dual-task performance. *Journal of Experimental Psychology, Human Perception and Performance*, v. 26, n. 4, p. 1260–1280, Aug. 2000.

LIMA, G. A. B. Interfaces entre a ciência da informação e a ciência cognitiva. *Ciência da Informação*, v. 32, n. 1, jan./abr. 2003. Disponível em: <http://www.ibict.br/cionline/320103/3210308.pdf>. Acesso em: 16 ago. 2003.

LINDUP, K. R. A new model for information security policies. *Computers & Security*, v. 14, n. 8, p. 691–695, Dec. 1995.

LISMONT, L.; MONGIN, P. Belief closure: a semantics of common knowledge for modal propositional logic. *Mathematical Social Sciences*, v. 30, n. 2, p. 127–153, Oct. 1995.

LITMAN, J. Ethical disobedience. *Ethics and Information Technology*, v. 5, n. 4, p. 217–223, 2003.

LIU, Q.; SAFAVI-NAINI, R.; SHEPPARD, N. P. Digital rights management for content distribution. In: *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*. Adelaide, Australia: Australian Computer Society, 2003. p. 49–58.

LOCH, K. D.; CONGER, S.; OZ, E. Ownership, privacy and monitoring in the workplace: a debate on technology and ethics. *Journal of Business Ethics*, v. 17, n. 6, p. 653–663, Apr. 1998.

LOHR, S.; MARKOFF, J. Windows is so slow, but why? *The New York Times*, 27 mar. 2006. Disponível em: <http://www.nytimes.com/2006/03/27/technology/27soft.html>. Acesso em: 28 mar. 2006.

LOPEZ, J.; OPPLIGER, R.; PERNUL, G. Authentication and authorization infrastructures (AAIs): a comparative survey. *Computers & Security*, v. 23, n. 7, p. 578–590, Oct. 2004.

LOWE, G. Towards a completeness result for model checking of security protocols. In: *Proceedings of the 11th Computer Security Foundations Workshop*. IEEE Computer Society, 1998. Disponível em: <http://citeseer.ist.psu.edu/460533.html>. Acesso em: 22 abr. 2004.

LÜBCKE, P. A semantic interpretation of Husserl's *epoché*: a debate on technology and ethics. *Synthese*, v. 118, n. 1, p. 1–12, Jan. 1999.

MADSEN, W. USA Patriot Act II: more snooping powers. *Network Security*, v. 2002, n. 11, p. 2, 2002.

MARCINCOWSKI, S. J.; STANTON, J. M. Motivational aspects of information security policies. In: *IEEE International Conference on Systems, Man and Cybernetics*. Oakland, California: IEEE Society, 2003. v. 3, p. 2527–2532.

MARCONDES, C. H.; JARDIM, J. M. Políticas de informação governamental: a construção do governo eletrônico na Administração Federal do Brasil. *DatagramaZero - Revista de Ciência da Informação*, v. 4, n. 2, Abr. 2003. Disponível em: <http://www.dgzero.org/abr03/Art_04.htm>. Acesso em: 5 junho 2003.

MARCOULATOS, I. Merleau-Ponty and Bourdieu on *Embodied Significance*. *Journal for the Theory of Social Behaviour*, v. 31, n. 1, Mar. 2001.

MARCOULATOS, I. John Searle and Pierre Bourdieu: Divergent perspectives on intentionality and social ontology. *Human Studies*, v. 26, n. 1, p. 67–96, Mar. 2003.

MARTINS, J. C. C. *Gestão de Projetos de Segurança da Informação*. Rio de Janeiro: Brasport, 2003.

MASUDA, Y. *A sociedade da informação*. Rio de Janeiro: Rio, 1982.

MATUS, C. Fundamentos da planificação situacional. In: ____. *Planejamento e Programação em Saúde*. São Paulo: Cortez, 1992. p. 105–149.

MAXWELL, T. A. The public need to know: emergencies, government organizations, and public information policies. *Government Information Quarterly*, v. 20, n. 3, p. 197–220, July 2003.

MAY, C. Dynamic corporate culture lies at the heart of effective security strategy. *Computer Fraud & Security*, v. 2003, n. 5, p. 10–13, May 2003.

MCGARRY, K. *O contexto dinâmico da informação*. Brasília: Briquet de Lemos, 1999.

MCINTOSH, A. *Using Information and Communication Technologies to Enhance Citizen Engagement in the Policy Process*. Paris: OECD, 2003.

MCLEAN, J. The algebra of security. In: *1988 IEEE Computer Society Symposium on Research on Security and Privacy*. Oakland, California: IEEE, 1988. p. 2–7.

MCLEAN, J. Security models and information flow. In: *1990 IEEE Computer Society Symposium on Research on Security and Privacy*. Oakland, California: IEEE, 1990. p. 180–187.

MCLEAN, J. The specification and modeling of computer security. *Computer*, v. 23, n. 1, p. 9–16, Jan. 1990.

MCLEAN, J. Reasoning about security models. In: *1997 IEEE Computer Society Symposium on Research on Security and Privacy*. Oakland, California: IEEE, 1997. p. 123–131. Disponível em: <http://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/mcLean_87.pdf>. Acesso em: 19 fev. 2005.

MCROBB, S.; ROBERSON, S. Are they really listening?: An investigation into published online privacy policies at the beginning of the third millenium. *Information Technology & People*, v. 17, n. 4, p. 442–461, 2004.

MEADOWS, C. Extending the Brewer-Nash model to a multilevel context. In: *IEEE Proceedings on Research on security and privacy*. Oakland, California: IEEE, 1990. p. 95–102.

MEADOWS, C.; MCLEAN, J. Security and dependability: then and now. In: *Proceedings on Computer Security, Dependability and Assurance: From Needs to Solutions*. Oakland, California: IEEE, 1998. p. 166–170.

MELO, M. A. Institutional choice and the diffusion of policy paradigms: Brazil and the second wave of pension reform. *International Political Science Review*, v. 25, n. 3, p. 320–341, July 2004.

MERALI, Y. The role of boundaries in knowledge processes. *European Journal of Information Systems*, v. 11, n. 1, p. 47–60, Mar. 2002.

MERCURI, R. T. Analyzing security costs. *Communications of the ACM*, v. 46, n. 6, p. 15–18, June 2003.

MERCURI, R. T. The HIPAA-potamus in health care data security. *Communications of the ACM*, v. 47, n. 7, p. 25–28, 2004. Disponível em: <http://doi.acm.org/10.1145/1005817.1005840>. Acesso em: 2 ago. 2004.

MERLEAU-PONTY, M. *Fenomenologia da Percepção*. Rio de Janeiro: Freitas Bastos, 1971.

MINGERS, J. Combining IS research methods: Towards a pluralist methodology. *Information Systems Research*, v. 12, n. 3, p. 240–259, Sept. 2001.

MINGERS, J. Embodying informations systems: the contribution of phenomenology. *Information and organization*, v. 11, n. 2, p. 103–128, Aug. 2001.

MINGERS, J. A classification of the philosophical assumptions of management science methods. *Journal of the Operational Research Society*, v. 54, n. 6, p. 559–570, June 2003.

MINGERS, J. Critical realism and information systems: brief responses to Monod and Klein. *Information and organization*, v. 14, n. 2, p. 145–153, Apr. 2004.

MINGERS, J. Real-izing information systems: critical realism as an underpinning philosophy for information systems. *Information and organization*, v. 14, n. 2, p. 87–103, Apr. 2004.

MINGERS, J.; BROCKLESBY, J. Multimethodology: towards a framework for mixing methodologies. *International Journal of Management Sciences*, v. 25, n. 5, p. 489–509, Oct. 1997.

MINISTÉRIO DA CIÊNCIA E TECNOLOGIA. *Livro Branco*: Ciência, tecnologia e inovação. Brasília: Ministério da Ciência e Tecnologia, 2002.

MIORA, M. Business continuity planning. In: BOSWORTH, S.; KABAY, M. (Eds.). *Computer Security Handbook*. 4th. ed. New York: John Wiley & Sons, 2002.

MIORA, M. Disaster recovery. In: BOSWORTH, S.; KABAY, M. (Eds.). *Computer Security Handbook*. 4th. ed. New York: John Wiley & Sons, 2002.

MIRANDA, A. *Ciência da Informação*: teoria de uma área em expansão. Brasília: Thesaurus, 2003.

MÓDULO SECURITY SOLUTIONS. 9ª *Pesquisa Nacional de Segurança da Informação*. Rio de Janeiro, 2003. Disponível em: <http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf>. Acesso em: 18 dez. 2003.

MORAHAN-MARTIN, J.; SCHUMACHER, P. Incidence and correlates of pathological internet use among college students. *Computers in Human Behavior*, v. 16, n. 1, p. 13–29, Jan. 2000.

MOTTA, J. R. C. G. da. *Análise de mercado*: tendências de investimento em segurança da informação no Brasil em 2004. Rio de Janeiro, 2004. Disponível em: <http://www.viaforum.com.br/admin/arq/SumarioExecutivo_SecurityWeek.pdf>. Acesso em: 9 abr. 2004.

MOULTON, R.; COLES, R. S. Applying information security governance. *Computers & Security*, v. 22, n. 7, p. 580–584, Oct. 2003.

MUIR, A.; OPPENHEIM, C. National Information Policy developments worldwide I: electronic government. *Journal of Information Science*, v. 28, n. 3, p. 173–186, June 2002.

MUIR, A.; OPPENHEIM, C. National Information Policy developments worldwide II: universal access - addressing the digital divide. *Journal of Information Science*, v. 28, n. 4, p. 263–273, Aug. 2002.

MUIR, A.; OPPENHEIM, C. National Information Policy developments worldwide III: e-commerce. *Journal of Information Science*, v. 28, n. 5, p. 357–373, Oct. 2002.

MUIR, A.; OPPENHEIM, C. National Information Policy developments worldwide IV: copyright, Freedom of Information and data protection. *Journal of Information Science*, v. 28, n. 6, p. 467–481, Dec. 2002.

MUNRO, A.; SUGDEN, R. On the theory of reference-dependent preferences. *Journal of Economic Behavior & Organization*, v. 50, n. 4, p. 407–428, Apr. 2003.

MYLES, J. F. From doxa to experience: issues in Bourdieu's adoption of husserlian phenomenology. *Theory, Culture & Society*, v. 21, n. 2, p. 99–107, Apr. 2004.

NAGRA, J.; THOMBORSON, C.; COLLBERG, C. A functional taxonomy for software watermarking. In: *Proceedings of the* 25^{th} *Australasian conference on Computer science*. Melbourne, Victoria, Australia: Australian Computer Society, 2002. p. 177–186.

NATIONAL INFORMATION ASSURANCE PARTNERSHIP. *Common Criteria for Information Technology Security Evaluation (ISO 15408) - v 2.2.*: Part 1 - introduction and general model. Washington, 2003. Disponível em: <http://www.commoncriteriaportal.org/public/files/ccpart1v2.2.pdf>. Acesso em: 9 jul. 2004.

NATIONAL INFORMATION ASSURANCE PARTNERSHIP. *Common Criteria for Information Technology Security Evaluation (ISO 15408) - v 2.2*: Part 2 - security functional requirements. Washington, 2003. Disponível em: <http://www.commoncriteriaportal.org/public/files/ccpart2v2.2.pdf>. Acesso em: 11 jul. 2004.

NATIONAL INFORMATION ASSURANCE PARTNERSHIP. *Common Criteria for Information Technology Security Evaluation (ISO 15408) - v 2.2*: Part 3 - security assurance requirements. Washington, 2003. Disponível em: <http://www.commoncriteriaportal.org/public/files/ccpart3v2.2.pdf>. Acesso em: 11 jul. 2004.

NBSO. *Site oficial do Network Information Center Security Office*. Rio de Janeiro, 2006. Disponível em: <http://www.nbso.nic.br/>. Acesso em: 25 jul. 2006.

NETWORK SECURITY. CPRM to protect movies and music. *Network Security*, v. 2001, n. 2, p. 3, Feb. 2001.

NEUMANN, P. G. Risks to the public in computers and related systems. *SIGSOFT Software Engineering Notes*, v. 29, n. 3, p. 7–14, 2004. Disponível em: <http://doi.acm.org/10.1145/986710.986716>. Acesso em: 2 ago. 2004.

NG, K. B. Toward a theoretical framework for understanding the relationship between situated action and planned action models of behavior in information retrieval contexts: contributions from phenomenology. *Information Processing and Management*, v. 38, n. 5, p. 613–626, Sept. 2002.

NIEUWENBURG, P. The agony of choice: Isaiah Berlin and the phenomenology of conflict. *Administration & Society*, v. 35, n. 6, p. 683–700, Jan. 2004.

NORTH, D. C. Institutions. *The Journal of Economic Perspectives*, v. 5, n. 1, p. 97–112, Winter 1991.

NUTT, P. C. Comparing public and private sector decision-making practices. *Journal of Public Administration Research and Theory*, Advance Access, p. 1–30, Mar. 2005.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Issues related to security of information systems and protection of personal data and privacy*. Paris, 1996. Disponível em: <http://www.oecd.org>. Acesso em: 6 maio 2003.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Electronic Commerce*. Paris, 2001. Disponível em: <http://www.oecd.org>. Acesso em: 17 fev. 2004.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Report on the OECD forum session on the privacy-enhandling technologies (PETs)*. Paris, 2001. Disponível em: <http://www.oecd.org>. Acesso em: 6 maio 2003.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Understading the digital divide*. Paris, 2001. Disponível em: <http://www.oecd.org/dataoecd/38/57/1888451.pdf>. Acesso em: 17 fev. 2004.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Using knowledge for development*: the brazilian experience. Paris, 2001. Disponível em: <http://www.oecd.org>. Acesso em: 6 maio 2003.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Civil Society and the OECD*. Paris, 2002. Disponível em: <http://www.oecd.org>. Acesso em: 17 fev. 2004.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Guidelines for the security of Information Systems and Networks*: towards a culture of security. Paris, 2002. Disponível em: <http://www.oecd.org/dataoecd/16/22/15582260.pdf>. Acesso em: 20 nov. 2002.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *OECD Information Technology Outlook*. Paris, 2002. Disponível em: <http://www.oecd.org/pdf/M00030000/M00030907.pdf>. Acesso em: 6 maio 2003.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *ICT Policy developments*. Paris, 2004. 285-328 p. Disponível em: <http://www.oecd.org>. Acesso em: 17 fev. 2004.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *OECD Official Site*. Paris, 2005. Disponível em: <www.ocde.org>. Acesso em: 2 jan. 2005.

ORMEROD, P. Complexity and the limits to knowledge. *Futures*, v. 37, n. 7, p. 721–728, Sept. 2005.

ORTALO, R. *Using deontic logic for security policy specification*. Toulouse, Oct. 1996. Disponível em: <http://dbserver.laas.fr/pls/LAAS/publis.rech_doc?langage=FR&clef=15965>. Acesso em: 2 maio 2003.

OSTROM, E. Institutional rational choice: an assessment of the institutional analysis and development frameworks. In: SABATIER, P. (Ed.). *Theories of the policy process*. Boulder - Colorado: Westview Press, 1999. p. 35–71.

PACHECO, R.; KERN, V. Arquitetura conceitual e resultados da integração de sistemas de informação e gestão da ciência e tecnologia. *DatagramaZero - Revista de Ciência da Informação*, v. 4, n. 2, 2003. Disponível em: <http://www.dgzero.org/abr03/Art_03.htm>. Acesso em: 5 junho 2003.

PARIKH, R.; RAMANUJAM, R. A knowledge based semantics of messages. *Journal of Logic, Language and Information*, v. 12, n. 4, p. 453–467, Sept. 2003.

PARIKH, R.; VÄÄNÄNEN, J. Finite information logic. *Annals of Pure and Applied Logic*, v. 134, n. 1, p. 83–93, June 2005.

PARSONS, W. *Public Policy*: an introduction to the theory and practice of policy analysis. Cheltenham, UK: Edward Elgar, 2001.

PASQUALI, L. (Org.). *Instrumentos psicológicos*: manual prático de elaboração. Brasília: LabPAMM, IBAPP, 1999.

PASQUALI, L. *Os tipos humanos*: A teoria da personalidade. Petrópolis: Vozes, 2003.

PASSY, F.; GIUGNI, M. Life-spheres, networks, and sustained participation in social movements: A phenomenological approach to political commitment. *Sociological Forum*, v. 15, n. 1, p. 117–144, Mar. 2000.

PASSY, F.; GIUGNI, M. Social networks and individual perceptions: Explaining differential participation in social movements. *Sociological Forum*, v. 16, n. 1, p. 123–153, Mar. 2001.

PAUL, A. T. Organizing Husserl: on the phenomenological foundations of Luhmann's systems theory. *Journal of Classical Sociology*, v. 1, n. 3, p. 371–394, Dec. 2001.

PAYNE, J. E. Regulation and information security: can Y2K lessons help us? *IEEE Security & Privacy*, v. 2, n. 2, p. 58–61, Mar./Apr. 2004.

PEMBLE, M. Balancing the security budget. *Computer fraud & security*, v. 2003, n. 10, p. 8–11, Oct. 2003.

PEMBLE, M. What do we mean by “information security”. *Computer fraud & security*, v. 2004, n. 5, p. 17–19, May 2004.

PETIT, J.-L. Between positivism and phenomenology: An exploration of the being of human being across transcendental phenomenology, analytic philosophy and the cognitive sciences. *Online originals*, 2003. Disponível em: <http://www.onlineoriginals.com/showitem.asp?itemID=287&articleID=12>. Acesso em: 4 maio 2005.

PFLEEGER, C. P. The fundamentals of information security. *IEEE Software*, v. 14, n. 1, p. 15–16,60, Jan./Feb. 1997.

PHUKAN, S.; DHILLON, G. Ethics and information technology use: a survey of US based SMEs. *Information Management & Computer Security*, v. 8, n. 5, p. 239–243, 2000.

PIERCEY, R. Ricoeur’s account of tradition and the Gadamer-Habermas debate. *Human Studies*, v. 27, n. 3, p. 259–280, Sept. 2004.

PIETARINEN, A.-V. What do epistemic logic and cognitive science have to do with each other? *Cognitive systems research*, v. 4, n. 3, p. 169–190, Sept. 2003.

PINHEIRO, W. *Projeto de Lei nº 6.525 de 2006*. Brasília, 2006.

PINTO, S. L. *A Política de Governo Eletrônico no Brasil*. Brasília, 2001. Disponível em: <http://www.governoeletronico.gov.br>. Acesso em: 19 maio 2003.

POSTHUMUS, S.; VON SOLMS, R. A framework for the governance of information security. *Computers & Security*, v. 23, n. 8, p. 638–646, Dec. 2004.

POTTER, B. Wireless security policies. *Network Security*, v. 2003, n. 10, p. 10–12, 2003.

PREECE, J.; NONNECKE, B.; ANDREWS, D. The top five reasons for lurking: improving community experiences for everyone. *Computers in Human Behavior*, v. 20, n. 2, p. 201–223, Mar. 2004.

PRESSMAN, R. S. *Software Engineering*: A practitioner’s approach. 2nd. ed. New York: McGraw-Hill, 1995.

PROJECT MANAGEMENT INSTITUTE. *PMBOK - Project Managenent Book of Knowledge*. Belo Horizonte: PMIMG, 2000. Disponível em: <www.pmimg.org.br/pdf/pmimg.pdf>. Acesso em: 15 fev. 2002.

PYLYSHYN, Z. Is vision continuous with cognition? The case for cognitive impenetrability of visual perception. *Behavioral and brain sciences*, v. 22, n. 3, p. 341–365, June 1999.

QUINN, A. C. Keeping the citizenry informed: early congressional printing and 21st century information policy. *Government Information Quarterly*, v. 20, n. 3, p. 281–293, July 2003.

RADFORD, G. P.; RADFORD, M. L. Structuralism, post-structuralism, and the library: de Saussure and Foucault. *Journal of Documentation*, v. 61, n. 1, p. 60–78, 2005.

RAGGAD, B. G. Corporate vital defense strategy: a framework for information assurance. In: *Proccedings of the 23rd National Information Systems Security Conference*. NIST-National Institute of Standards and Technology, 2000. Disponível em: <http://csrc.nist.gov/nissc/2000/proceedings/papers/029.pdf>. Acesso em: 9 jul. 2003.

RAJAN, R. G.; ZINGALES, L. The tyranny of inequality. *Journal of Public Economics*, v. 76, n. 3, p. 521–558, June 2000.

RAMANUJAM, R.; SURESH, S. P. Information based reasoning about security protocols. *Electronic Notes on Theorical Computer Sciences*, v. 55, n. 1, p. 1–16, Jan. 2003.

RATNER, R. K.; HERBST, K. C. When good decisions have bad outcomes: The impact of affect on switching behavior. *Organizational Behavior and Human Decision Processes*, v. 96, n. 1, p. 23–37, Jan. 2005.

REGAN, P. M. Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly*, v. 21, n. 4, p. 481–497, 2004.

RELYEA, H. C. Homeland security and information. *Government Information Quarterly*, v. 19, n. 3, p. 213–233, 2002.

RHODEN, E. People and processes: the key elements to information security. *Computer Fraud & Security*, v. 6, n. 1, p. 14–15, June 2002.

RICOEUR, P. Phenomenology and hermeneutics. *Noûs*, v. 9, n. 1, p. 85–102, Apr. 1975.

RICOEUR, P. *Hermeneutics and the human sciences*. Cambridge: Cambridge University Press, 1982.

RICOEUR, P. *Interpretação e ideologias*. 4a. ed. Rio de Janeiro: Francisco Alves, 1990. Organização, tradução e apresentação de Hilton Japiassu.

RICOEUR, P. *O si-mesmo como um outro*. São Paulo: Papirus, 1991.

RISSER, J. Hermeneutics between Gadamer and Heidegger. *Philosophy Today*, v. 41, p. 134–141, 1997.

RIST, R. C. Influencing the policy process with qualitative research. In: DENZIN, N. K.; LINCOLN, Y. S. (Eds.). *Handbook of qualitative research*. 2. ed. Thousand Oaks - California: Sage, 2000. p. 1001–1017.

ROBBINS, S. P. *Comportamento Organizacional*. 9a. ed. São Paulo: Prentice Hall, 2002.

ROCHET, C. Rethinking the management of information in the strategic monitoring of public policies by agencies. *Industrial Management & Data Systems*, v. 104, n. 3, p. 201–208, 2004.

ROSE, R. A global diffusion model of e-governance. *Journal of Public Policy*, v. 25, n. 1, p. 5–27, May 2005.

ROSENBERG, V. Information policies of developing countries: the case of Brazil. *Journal of the American Society for Information Science*, v. 33, n. 4, p. 203–207, July 1982.

RUBINSTEIN, J. S.; MEYER, D. E.; EVANS, J. E. Executive control of cognitive processes in task switching. *Journal of Experimental Psychology, Human Perception and Performance*, v. 27, n. 4, p. 763–797, Aug. 2001.

RYAN, L. V. Corporate governance and business ethics in North America: the state of the art. *Business & Society*, v. 44, n. 1, p. 40–73, Mar. 2005.

SABATIER, P. A. Toward better teories of the policy process. *PS: Political Science and Politics*, v. 24, n. 2, p. 147–156, June 1991.

SADALA, M. L. A.; ADORNO, R. de C. F. Phenomenology as a method to investigate the experience lived: a perspective from Husserl and Merleau Ponty's thought. *Journal of Advanced Nursing*, v. 37, n. 3, p. 282–293, Feb. 2002.

SAGA. *Standards and Architectures for e-Government Applications - v. 2*. Munique, 2004. Disponível em: <http://www.kbst.bund.de/Anlage304417/Saga_2_0_en_final.pdf>. Acesso em: 8 abr. 2004.

SALTZER, J. H.; SCHROEDER, M. D. The protection of information in computer systems. *Proceedings of the IEEE*, v. 63, n. 9, p. 1278–1308, Sept. 1975. Disponível em: <http://www.acsac.org/secshelf/papers/protection_information.pdf>. Acesso em: 30 jul. 2004.

SAMUELSON, P. DRM {and, or, vs} the law. *Communications of the ACM*, v. 46, n. 4, p. 41–45, Apr. 2003.

SANDERS, P. Phenomenology: a new way of viewing organizational research. *The Academy of Management Review*, v. 7, n. 3, p. 353–360, July 1982.

SANDHU, R. S. et al. Role based access control models. *Computer*, v. 29, n. 2, p. 38–47, Feb. 1996.

SANS. *Email use policy*. Bethesda, Maryland, 2002. Disponível em: <http://www.sans.org/resources/policies/Email_Policy.pdf>. Acesso em: 12 mai. 2003.

SANS. *The Twenty Most Critical Internet Security Vulnerabilities*. Bethesda, Maryland, 2004. Disponível em: <http://files.sans.org/top20.pdf>. Acesso em: 10 dez. 2004.

SARACEVIC, T. Interdisciplinary nature of information science. *Ciência da Informação*, v. 24, n. 1, p. 36–40, 1995. Disponível em: <http://www.ibict.br/cionline/240195/24019505.pdf>. Acesso em: 19 ago. 2003.

SARACEVIC, T. Information science. *Journal of the American Society for Information Science*, v. 50, n. 12, p. 1051–1063, Oct. 1999.

SASSE, M. A.; BROSTOFF, S.; WEIRICH, D. Transforming the 'weakest link': a human/computer interaction approach to usable and effective security. *BT Technology Journal*, v. 19, n. 3, p. 122–131, July 2001.

SCHABRACQ, M. J.; COOPER, C. L. Toward a phenomenological framework for the study of work and organizational stress. *Human Relations*, v. 51, n. 5, p. 625–648, May 1998.

SCHEIN, E. *Organizational culture and leadership*. 2. ed. San Francisco: Jossey-Bass, 1992.

SCHELL, R. R. Information security: science, pseudoscience and flying pigs. In: 17^{th} *Computer Security Applications Conference*. [S.l.]: ACSAC, 2001. p. 205–216.

SCHLIENGER, T.; TEUFEL, S. Analyzing information security culture: increased trust by an appropriate information security culture. In: *Proceedings of the* 14^{th} *International Workshop on Database and Expert Systems Applications*. Oakland, California: IEEE Society, 2003. v. 6, p. 405–409.

SCHMIDT, D. J. On the significance of nature for the question of ethics. *Research in Phenomenology*, v. 31, p. 62–77, 2001.

SCHMIDT, R. H.; SPINDLER, G. Path dependence, corporate governance and complementarity. *International Finance*, v. 5, n. 2, p. 311–333, Nov. 2002.

SCHMITTER, P. C. Reflexões sobre o conceito de política. In: ____. *Curso de Introdução à Ciência Política - Unidade I*. Brasília: UnB, 1982. p. 29–35.

SCHNEIDER, F. B. Enforceable security policies. *ACM Transactions on Information and Systems Security*, v. 3, n. 1, p. 30–50, Feb. 2000.

SCHNEIER, B. *Applied Cryptography*. New York: John Wiley & Sons, 1996.

SCHNEIER, B. *Secrets and Lies*: digital security in a networked world. New York: John Wiley & Sons, 2000.

SCHULTZ, E. E. A framework for understanding and predicting insider attacks. *Computers & Security*, v. 21, n. 6, p. 526–531, Oct. 2002.

SCHULTZ, E. E. Information security and the media. *Computers & Security*, v. 22, n. 8, p. 652–653, Dec. 2003.

SCHULTZ, E. E. Sarbanes-Oxley: a huge boon to information security in the US. *Computers & Security*, v. 23, n. 5, p. 353–354, July 2004.

SELDÉN, L. On Grounded Theory? With some malice. *Journal of Documentation*, v. 61, n. 1, p. 114–129, 2005.

SELKER, T. Fixing the vote. *Scientific American*, v. 291, n. 4, p. 60–67, Oct. 2004.

SÊMOLA, M. *Gestão da segurança da informação*: uma visão executiva. Rio de Janeiro: Campus, 2003.

SERJANTOV, A.; ANDERSON, R. On dealing with adversaries fairly. In: 3^{rd} *Annual Workshop on Economics of Information Security*. University of Minnesota, 2004. Disponível em: <http://www.dtc.umn.edu/weis2004/serjantov.pdf>. Acesso em: 30 jul. 2004.

SHANNON, C. E. A matemathical theory of communication. *The Bell System Technical Journal*, v. 27, n. 1, p. 379–423;623–656, July/Oct. 1948. Disponível em: <http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf>. Acesso em: 21 maio 2004.

SHANNON, C. E.; WEAVER, W. *Teoria matemática da comunicação*. São Paulo: Difel, 1975.

SHAO, M.-H.; HWANG, J.-J.; WU, S. A transactional-cycle approach to evidence management for dispute resolution. *Information & Management*, v. 42, n. 4, p. 607–618, May 2005.

SHAPIRO, B.; BAKER, C. R. Information technology and the social construction of information privacy. *Journal of Accounting and Public Policy*, v. 20, n. 4-5, p. 295–322, Winter 2001.

SHAPIRO, C. *A economia da informação*: Como os princípios econômicos se aplicam à era da internet. 4. ed. Rio de Janeiro: Campus, 1999.

SHARPE, A.; RUSSELL, C. Private rights and public policy. *Computer Law & Security Report*, v. 19, n. 5, p. 411–415, Sept. 2003.

SHIREY, R. *RFC 2828 - Internet Security Glossary*. 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt>. Acesso em: 2 maio 2003.

SHULER, J. A. Citizen-centered government: Information policy possibilities for the 108th congress. *Journal of Academic Librarianship*, v. 29, n. 2, p. 107–110, Feb. 2003.

SHULOCK, N. The paradox of policy analysis: If it is not used, why do we produce so much of it? *Journal of Policy Analysis and Management*, v. 18, n. 2, p. 226–244, 1999.

SIPONEN, M. T. Five dimensions of information security awareness. *ACM Computers and Society*, v. 31, n. 2, p. 24–29, June 2001.

SIPONEN, M. T. Analysis of moderm IS security development approaches: towards the next generation of social and adaptable iss developments. *Information and Organization*, v. 15, n. 4, p. 339–375, Oct. 2005.

SKOULARIDOU, V.; SPINELLIS, D. Security architectures for network clients. *Information Management & Computer Security*, v. 11, n. 2, p. 84–91, 2003.

SKRAPEC, C. A. Phenomenology and serial murder: asking different questions. *Homicide Studies*, v. 5, n. 1, p. 46–63, 2001.

SLEEMAN, B. Recent literature on government information. *Journal of Government Information*, v. 30, n. 1, p. 20–41, 2004.

SMITH, G. W.; NEWTON, R. B. A taxonomy of organisational security policies. In: *Proccedings of the 23rd National Information Systems Security Conference*. NIST-National Institute of Standards and Technology, 2000. Disponível em: <http://csrc.nist.gov/nissc/2000/proceedings/papers/052.pdf>. Acesso em: 4 jul. 2003.

SMITH, K. B. Typologies, taxonomies, and the benefits of policy classification. *Policy Studies Journal*, v. 30, n. 3, p. 379–395, Aug. 2002.

SMITH, R. E. Experimenting with security policy. In: 2nd *DARPA Information Survivability Conference & Exposition*. Washington: DARPA, 2001. v. 1, p. 116–122.

SOBEL, A. E. K.; ALVES-FOSS, J. A trace-based model of the chinese wall security policy. In: *Proceedings of the 22nd National Information Systems Security Conference*. NIST-National Institute of Standards and Technology, 1999. Disponível em: <http://csrc.nist.gov/nissc/1999/proceeding/papers/p9.pdf>. Acesso em: 19 fev. 2005.

SPILLER, P. T.; TOMMASI, M. The institutional foundations of public policy: a transactions approach with application to Argentina. *Journal of Law, Economics, & Organization*, v. 19, n. 2, p. 281–306, Oct. 2003.

SPURLING, P. Promoting security awareness and commitment. *Information Management & Computer Security*, v. 3, n. 2, p. 20–26, 1995.

STANTON, J. M. et al. Examining the linkage between organizational commitment and information security. In: *IEEE International Conference on Systems, Man and Cybernetics*. Oakland, California: IEEE Society, 2003. v. 3, p. 2501–2506.

STANTON, J. M. et al. Analysis of end user security behaviors. *Computers & Security*, v. 24, n. 2, p. 124–133, Mar. 2005.

STEGMÜLLER, W. *A filosofia contemporânea*: introdução crítica. São Paulo: EdUSP, 1977.

STEIN, E. et al. *The Politics of policies*: Economic and social progress in Latin America. Washington, 2005. Disponível em: <http://www.iadb.org/res/ipes/2006/index.cfm?language=english>. Acesso em: 15 jan. 2006.

STEINER, P. Dogs on the web. *The New Yorker*, v. 69, n. 20, p. 61, July 1993. Charge.

STEPHENSON, P. Using formal modeling to untangle security incidents. *Computer Fraud & Security*, v. 2004, n. 7, p. 17–20, July 2004.

STERGIOU, T.; LEESON, M.; GREEN, R. An alternative architectural framework to the OSI security model. *Computers & Security*, v. 23, n. 2, p. 137–153, Mar. 2004.

STEWART, A. On risk: perception and direction. *Computers & Security*, v. 23, n. 5, p. 362–370, July 2004.

STRAUB, D. *Computer Abuse Questionnaire*. 1990. Disponível em: <http://www.ucalgary.ca/newsted/∼q5200.htm>. Acesso em: 31 ago. 2004.

STRAUSS, J.; ROGERSON, K. S. Policies for online privacy in the United States and the European Union. *Telematics and Informatics*, v. 19, n. 2, p. 173–192, May 2002.

SUNDIN, O.; JOHANNISSON, J. Pragmatism, neo-pragmatism and sociocultural theory: communicative participation as a perspective in LIS. *Journal of Documentation*, v. 61, n. 1, p. 23–43, 2005.

SYVERSON, P. F.; GRAY, J. W. The epistemic representation of information flow security in probabilistic systems. In: *Proceedings of the* 8^{th} *IEEE Computer Security Foundations Workshop*. Oakland, California: IEEE, 1995. p. 152–166.

TAKAHASHI, T. *Sociedade da Informação no Brasil*: Livro verde. Brasília: Ministério da Ciência e Tecnologia, 2000.

TALJA, S.; TUOMINEN, K.; SAVOLAINEN, R. “Isms” in information science: constructivism, collectivism and constructionism. *Journal of Documentation*, v. 61, n. 1, p. 79–101, 2005.

TAMURA, H. Behavioral models for complex decision analysis. *European Journal of Operational Research*, v. 166, n. 3, p. 655–665, Nov. 2005.

TANAKA, H.; MATSUURA, K.; SUDOH, O. Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy*, v. 24, n. 1, p. 37–59, Jan./Feb. 2005.

TASSEY, G. Policy issues for R&D investment in a knowledge-based economy. *Journal of Technology Transfer*, v. 29, n. 2, p. 29–38, Apr. 2004.

TAYLOR, C. To follow a rule... In: CALHOUN, C.; LIPUMA, E.; POSTONE, M. (Eds.). *Bourdieu*: Critical perspectives. Chicago: Chicago University, 1993. p. 150–165.

TELEFÔNICA. *Sociedade da Informação no Brasil*: Presente e perspectivas. São Paulo: Grupo Telefônica, 2002. Disponível em: <http://www.telefonica.es/sociedaddelainformacion/brasil2002/#>. Acesso em: 17 fev. 2004.

THIAGARAJAN, V. *Information Security Management*: BS 7799.2:2002 Audit Check List. Bethesda, Maryland, 2003. Disponível em: <http://www.sans.org/score/checklists/ISO_17799_checklist.pdf>. Acesso em: 3 ago. 2004.

THOMAS, L. *Autonomy, behavior & moral goodness*. 2002. Disponível em: <http://cogprints.ecs.soton.ac.uk/archive/00003015/01/Autonomy.pdf>. Acesso em: 25 jun. 2004.

THOMSON, M. *Making information security awareness and training more effective*. 2001. Disponível em: <citeseer.ist.psu.edu/458025.html>. Acesso em: 6 mar. 2005.

THORNTON, J.; WHITE, A. A heideggerian investigation into the lived experience of humour by nurses in an intensive care unit. *Intensive and Critical Care Nursing*, v. 15, n. 5, p. 266–278, Oct. 1999.

THROOP, C. J.; MURPHY, K. M. Bourdieu and phenomenology: a critical assessment. *Anthropological theory*, v. 2, n. 2, p. 185–207, June 2001.

TINGLING, P.; PARENT, M. An exploration of enterprise technology selection and evaluation. *Journal of Strategic Information Systems*, v. 13, n. 4, p. 329–354, Dec. 2004.

TIROLE, J. Corporate governance. *Econometrica*, v. 69, n. 1, p. 1–35, Jan. 2001.

TONG, C. K. S. et al. Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard. *International Congress Series*, v. 1256, p. 311–318, 2003.

TORLAK, G. N. Reflections on multimethodology: Maximizing flexibility, responsiveness, and sustainability in multimethodology interventions through a theoretically and practically improved version of total systems intervention (TSI). *Systemic Practice and Action Research*, v. 14, n. 3, p. 297–337, June 2001.

TROMPETER, C. M.; ELOFF, J. H. P. A framework for the implementation of socio-ethical controls in information security. *Computers & Security*, v. 20, n. 5, p. 384–391, July 2001.

TRYFONAS, T.; KIOUNTOUZIS, E.; POULYMENAKOU, A. Embedding security practices in contemporary information systems development approaches. *Information Management & Computer Security*, v. 9, n. 4, p. 183–197, 2001.

TSOUMAS, V.; TRYFONAS, T. From risk analysis to effective security management: towards an automated approach. *Information Management & Computer Security*, v. 12, n. 1, p. 91–101, 2004.

TURNBUL, S. The science of corporate governance. *Corporate Governance*, v. 10, n. 4, p. 261–277, Oct. 2002.

TURNER, J. M.; MOAL, V. *Metrométa*. Montréal, 2003. Disponível em: <http://mapageweb.umontreal.ca/turner/meta/francais/metrometa.html>. Acesso em: 9 fev. 2004.

UK DEPARTMENT OF TRADE AND INDUSTRY. *Data Security*: Technology and the law. Londres, 2004. Disponível em: <http://www.dti.gov.uk/bestpractice/assets/security/elaw.pdf>. Acesso em: 29 jul. 2004.

UK DEPARTMENT OF TRADE AND INDUSTRY. *Data Security*: Legislation factsheet. Londres, 2004. Disponível em: <http://www.dti.gov.uk/bestpractice/assets/security/legislation.pdf>. Acesso em: 29 jul. 2004.

UK DEPARTMENT OF TRADE AND INDUSTRY. *Information Security*: Bs7799 and the data protection act. Londres, 2004. Disponível em: <http://www.dti.gov.uk/bestpractice/assets/security/dpa.pdf>. Acesso em: 29 jul. 2004.

UK DEPARTMENT OF TRADE AND INDUSTRY. *Information Security*: Hard facts. Londres, 2004. Disponível em: <http://www.dti.gov.uk/bestpractice/assets/hardfacts.pdf>. Acesso em: 29 jul. 2004.

UNIÃO EUROPÉIA. *Site oficial*. Bruxelas, 2003. Disponível em: <www.eu.int>. Acesso em: 9 maio 2003.

UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION. *Country profiles of e-governance*. Paris, 2002.

US CENSUS BUREAU OF THE DEPARTMENT OF COMMERCE. *Quarterly retail e-commerce sales*: 4th quarter 2005. Washington - DC, 2006. Disponível em: <http://www.census.gov/mrts/www/data/html/05Q4.html>. Acesso em: 9 maio 2006.

VAN DER HAAR, H.; VON SOLMS, R. A model for deriving information security control attribute profiles. *Computers & Security*, v. 22, n. 3, p. 233–244, Apr. 2003.

van der Hoek, W.; WOOLDRIDGE, M. Model checking cooperation, knowledge, and time: a case study. *Research in Economics*, v. 57, n. 3, p. 235–265, Sept. 2003.

VANDENBERGHE, F. The nature of culture: Towards a realist phenomenology of material, animal and human nature. *Journal for the Theory of Social Behaviour*, v. 33, n. 4, p. 461–475, Dec. 2003.

VANN, J. L. Resistance to change and the language of public organizations: a look at “clashing grammars” in large-scale information technology projects. *Public Organization Review*, v. 4, n. 1, p. 47–73, Mar. 2004.

VARELA, F. J.; THOMPSON, E.; ROSCH, E. *The embodied mind*: cognitive science and human experience. Cambridge, Massachusetts: MIT Press, 1993.

VENTER, H. S.; ELOFF, J. H. P. A taxonomy for information security technologies. *Computers & Security*, v. 22, n. 4, p. 299–307, May 2003.

VENTER, H. S.; ELOFF, J. H. P. Vulnerability forecasting: a conceptual model. *Computers & Security*, v. 23, n. 6, p. 489–497, Sept. 2004.

VERMEULEN, C.; VON SOLMS, R. The information security management toolbox: taking the pain out of security management. *Information Management & Computer Security*, v. 10, n. 3, p. 119–125, 2002.

VILLELA-PETIT, M. Narrative identity and ipseity by Paul Ricoeur: from Ricoeur's ‘Time and Narrative’ to ‘Oneself as an Other’. *Online originals*, 2003. Disponível em: <http://www.onlineoriginals.com/showitem.asp?itemID=286>. Acesso em: 4 maio 2005.

VOLKMAN, R. Privacy as life, liberty, property. *Ethics and Information Technology*, v. 5, n. 4, p. 199–210, 2003.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management. *Computers & Security*, v. 23, n. 5, p. 371–376, July 2004.

VON SOLMS, R. Information security management: why standards are important. *Information Management & Computer Security*, v. 7, n. 1, p. 50–57, 1999.

VON SOLMS, R.; VON SOLMS, B. From policies to culture. *Computers & Security*, v. 23, n. 4, p. 275–279, June 2004.

VRANAS, P. B. M. Gigerenzer's normative critique of Kahneman and Tversky. *Cognition*, v. 76, n. 3, p. 179–193, Sept. 2000.

VROOM, C.; VON SOLMS, R. Towards information security behavioural compliance. *Computers & Security*, v. 23, n. 3, p. 191–198, May 2004.

WALDRON, J. *Moral autonomy and personal autonomy*. Filadelfia, 2002. Disponível em: <http://philosophy.la.psu.edu/jchristman/autonomy/Waldron.pdf>. Acesso em: 10 jun. 2004.

WALLISER, B. Epistemic logic and game theory. In: BICCHIERI, C.; CHIARA, M. L. D. (Eds.). *Knowledge, belief, and strategic interaction*. New York: Cambridge University Press, 1992. p. 197–226.

WALTON, J. P. Developing an enterprise information security policy. In: *Proceedings of the 30th annual ACM SIGUCCS conference on User services*. Providence, Rhode Island, USA: ACM, 2002. p. 153–156. Disponível em: <http://doi.acm.org/10.1145/588646.588678>. Acesso em: 2 ago. 2004.

WANG, H.; WANG, C. Taxonomy of security considerations and software quality: addressing security threats and risks through software quality design factors. *Communications of the ACM*, v. 46, n. 6, p. 75–78, June 2003.

WEIMER, J.; PAPE, J. C. A taxonomy of systems of corporate governance. *Corporate Governance*, v. 7, n. 2, p. 152–166, Apr. 1999.

WERSIG, G. Information science: the study of postmodern knowledge usage. *Information Processing & Management*, v. 29, n. 2, p. 229–239, Mar./Apr. 1993.

WHITE, J. D. Phenomenology and organization development. *Public Administration Quarterly*, v. 14, n. 1, p. 76–85, Spring 1990.

WHITMAN, M. E. Enemy at the gate: threats to information security. *Communications of the ACM*, v. 46, n. 8, p. 91–95, Aug. 2003.

WIKGREN, M. Critical realism as a philosophy and social theory in information science? *Journal of Documentation*, v. 61, n. 1, p. 11–22, 2005.

WIKLUND, L.; LINDHOLM, L.; LINDSTRÖM, U. Å. Hermeneutics and narration: a way to deal with qualitative data. *Nursing Inquiry*, v. 9, n. 2, p. 114–125, June 2002.

WILLIAMS, P. Information security governance. *Information security technical report*, v. 6, n. 3, p. 60–70, Nov. 2001.

WILLIS, C. E. The phenomenology of pornography: a comment on Catharine MacKinnon's *Only Words*. *Law and Phylosophy*, v. 16, n. 2, p. 177–199, Jan. 2003.

WILSON, C. A. Policy regimes and policy change. *Journal of Public Policy*, v. 20, n. 3, p. 247–274, Dec. 2000.

WILSON, P. Technical challenges faced when companies merge... *Network Security*, v. 2004, n. 5, p. 5–7, May 2004.

WILSON, T. Exploring models of information behaviour: the 'uncertainty' project. *Information Processing and Management*, v. 35, n. 6, p. 839–849, Nov. 1999.

WILSON, T. D. Alfred Schutz, phenomenology and research methodology for information behaviour research. 2002. Disponível em: <http://informationr.net/tdw/publ/papers/schutz02.html>. Acesso em: 24 maio 2005.

WILSON, T. D. Philosophical foundations and research relevance: issues for information research. *Journal of Information Science*, v. 29, n. 6, p. 445–452, Dec. 2003.

WILSON, T. P. Conceptions of interaction and forms of sociological explanation. *American Sociological Review*, v. 35, n. 4, p. 697–710, Aug. 1970.

WOOD, C. C. An unnapreciated reason why information security policies fail. *Computer Fraud & Security*, v. 2000, n. 10, p. 13–14, Oct. 2000.

WOOD, C. C. Don't let the role of information security policies in the Arthur Andersen/Enron case go without mention to your Chief Executive Officer. *Computer Fraud & Security*, v. 2002, n. 5, p. 11–13, May 2002.

WOOD, C. C. *Information Security Policies Made Easy*: Version 9. Boston: Baseline Software Press, 2002.

WOOD, C. C. Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*, v. 2004, n. 1, p. 16–17, Jan. 2004.

WOOD, C. C.; PARKER, D. B. Why ROI and similar financial tools are not advisable for evaluating the merits of security projects. *Computer Fraud & Security*, v. 2004, n. 5, p. 8–10, May 2004.

XENITELLIS, S. D. Identifying security vulnerabilities through input flow tracing and analysis. *Information Management & Computer Security*, v. 11, n. 4, p. 195–199, 2003.

YANG, J.; QIU, W. A measure of risk and a decision-making model based on expected utility and entropy. *European Journal of Operational Research*, v. 164, n. 3, p. 792–799, Aug. 2005.

ZHANG, C. N.; YANG, C. Information flow analysis on role-based access control model. *Information Management & Computer Security*, v. 10, n. 5, p. 225–236, 2002.

ZHANG, P.; LI, N. An assessment of human computer interaction research in management information systems: topics and methods. *Computers in Human Behavior*, v. 20, n. 2, p. 125–147, Mar. 2004.

ZUCCATO, A. Holistic security requirement engineering for electronic commerce. *Computers & Security*, v. 23, n. 1, p. 63–76, Feb. 2004.

ZURKO, M. E.; SIMON, R. T. User-centered security. In: *Proceedings of the 1996 workshop on new security paradigms*. Lake Arrowhead, California: ACM, 1996. v. 1, n. 1, p. 27–33.

Glossário

Autoridade Certificadora

Organismo responsável pela autenticação dos participantes de uma rede de assinatura digital por chave pública.

Criptografia

Processo de cifragem (embaralhamento) dos dados de modo tal a permitir que apenas os conhecedores da chave associada sejam capazes de reverter o processo e ter acesso ao conteúdo em texto pleno.

Criptografia de chaves públicas

Processo de criptografia no qual a cifragem e a decifragem baseiam-se em um par de chaves: uma delas, a chave privada, é de posse exclusiva do autor, ao passo que a outra, a chave pública, é disseminada aos participantes da rede.

Criptografia de chaves simétricas

Processo de criptografia no qual a cifragem e a decifragem baseiam-se em uma mesma chave.

Engenharia social

Técnica do uso de subterfúgios usados como persuasão e voltados a obter acesso a informações privilegiadas por meio de pessoas direta ou indiretamente relacionadas ao possuidor dos meios legítimos de acesso.

Firewall

Elemento de software destinado a filtrar o acesso a uma rede privativa, isolando-a da rede pública.

Framework

Conjunto de métodos e técnicas destinados a representar, verificar e validar determinado modelo.

Hacking

Acesso não autorizado a bases de dados ou a redes de telecomunicações, acompanhado ou não da coleta de conteúdo armazenado ou trafegado.

Rede ponto a ponto

Rede cujos nós (elementos) têm prioridades semelhantes de acesso e de uso de recursos. Distinguem-se das redes hierárquicas pela ausência de um servidor dedicado ou outros nós preponderantes.

Security officer

Pessoa responsável pela segurança da informação em ambientes organizacionais.

APÊNDICE A – Psicologia e segurança da informação

A.1 Introdução

Os seguintes conceitos abordados por este domínio do conhecimento são de particular interesse para a segurança da informação:

- Tipologia da personalidade;
- Percepção do conceito de segurança e as ações determinadas por esta percepção;
- Análise do comportamento;
- Aspectos individuais dos atores humanos e sua caracterização frente ao grupo (organização); e
- Construção, validação e aplicação de instrumentos de aferição da percepção.

Por meio da formulação de instrumentos (questionários e/ou entrevistas), objetiva-se captar a percepção dos usuários, em todos os níveis organizacionais, perante o tema "segurança da informação". A construção de instrumentos adequados segue a estrutura e o formalismo de itens de medida psicológicos que se encontram adequadamente testados e validados. O motivo para a construção e aplicação destes instrumentos é o distanciamento observado entre as expectativas que norteiam a implementação das políticas e a real preparação dos usuários para o comportamento voltado à segurança, o qual é, por muitas vezes, contrário às práticas usuais - como exemplo, cite-se a exigência de realização periódica de cópia de segurança (*backup*) dos dados institucionais de posse do usuário. Desta forma, almeja-se reduzir a lacuna entre o comportamento usualmente apresentado e o comportamento almejado.

A.2 Teoria psicológica

Segundo Pasquali (2003), os instrumentos sensoriais ou habilidades que se manifestam pelo comportamento humano distinguem-se nas categorias dispostas na Tabela 9.

SER	Conhecer	Sentir	Agir
Físico	*Sentidos* tato olfato visão audição paladar	*Sistema neuro-endócrino*	*Instinto* alerta sobrevivência reprodução exploração proteção
Psíquico	*Intelecto* memória percepção imaginação intuição raciocínio	*Senso de valor* estético ético grande (?) mágico (?) ...	*Vontade* atenção escolha significado da vida ... ...

Tabela 9: Teoria da personalidade [adaptada de Pasquali (2003, p. 56-57)].

Este modelo propõe que a personalidade seja composta por duas esferas, a física e a psíquica (Pasquali (2003) sugere ainda a existência da esfera espiritual, mas não a aborda). Em ambas as esferas, manifestam-se construtos do comportamento, divididos em três grandes categorias: o conhecer, o sentir e o agir. Na interseção entre a esfera psíquica e a categoria do conhecer, encontra-se, entre outros construtos, a percepção, objeto do interesse da segurança da informação.

Desta forma, um instrumento deverá medir este aspecto. Cumpre observar que o instrumento não visa a estabelecer diferenciações entre a segurança da informação “percebida” e a segurança da informação “real”, como é usual em instrumentos para a aferição do risco, como o mostrado, por exemplo, em Jasanoff (1998). Pretende-se medir especificamente a percepção dos usuários do que seja a segurança da informação, na acepção por eles vivenciada.

A.2.1 A teoria da percepção

A teoria da percepção tem estado ligada, historicamente, aos sentidos (RUBINSTEIN; MEYER; EVANS, 2001), principalmente à visão (DAVIDOFF, 1983), embora haja questões em aberto quanto à associação entre visão e cognição (PYLYSHYN, 1999). Perguntas ligadas ao reconhecimento de cores, sons, aromas, texturas e sabores sempre permearam os estudos sobre este tema. Como o homem é capaz de perceber o ambiente à sua volta, e qual o grau de

exatidão do que ele percebe? No tocante às ciências, cumpre lembrar que, à parte o aparato tecnológico de que se dispõe atualmente, é a percepção do cientista que constitui o objeto de todos os campos de estudo. É o seu olho que se posiciona na lente do microscópio ou que observa as imagens de satélite, e, mesmo que se use um computador para analisar estas imagens, o resultado desta análise é submetido ao escrutínio (em geral, ao olhar) do pesquisador. Deste modo, o conhecimento do mundo é dependente dos sentidos, e eis o motivo fundamental para o seu estudo. Deve-se diferenciar os sentidos, existentes na esfera física, do seu processamento por meio do intelecto, contido no domínio da esfera psíquica (vide a Tabela 9).

A facilidade com que se usam os sentidos mascara o fato de que a percepção é uma atividade cerebral extremamente complexa (COREN; WARD, 1989). Os processos perceptivos recuperam dados armazenados na mente, requerendo classificações e comparações sutis, além de uma ampla gama de decisões antes que a consciência se dê conta de que "há algo lá". Como um exemplo, cite-se o fato de que não são os olhos que vêem: há milhares de pessoas que possuem olhos perfeitamente funcionais, sem que haja impressões sensoriais da visão, e que não podem ver por terem lesões nas porções do cérebro que recebem e interpretam as mensagens vindas do aparelho visual.

A teoria indica que não há uma linha clara entre a percepção e muitas outras atividades comportamentais (LIEN; PROCTOR, 2000; RUBINSTEIN; MEYER; EVANS, 2001). A percepção, por si só, não é capaz de prover um conhecimento direto do mundo, que é o produto final de uma série de processos.

Pode-se definir o estudo da percepção como o estudo da experiência consciente dos objetos e das relações entre estes objetos (COREN; WARD, 1989). Num sentido mais amplo, ao estudo da percepção interessa como se forma uma representação consciente do ambiente externo, e qual a acurácia desta representação.

Outro conceito um pouco mais recente no campo da psicologia da percepção é o de *processamento da informação* (BARBER; LEGGE, 1976). Esta abordagem enfatiza como a informação a respeito do mundo externo é processada a fim de produzir a percepção consciente e guiar as ações do indivíduo. Tipicamente, este conceito inclui a fase sensorial ou de registro, a fase interpretativa ou de percepção, e uma fase cognitiva ou de memória, integrando assim estes três conceitos. Novamente, a linha divisória entre estes temas se mostra tênue.

Do mesmo modo que se apresentam diversos aspectos da percepção, igualmente se apresentam diferentes abordagens teóricas dos problemas a ela relativos. Uma destas abordagens é o *reducionismo biológico*, baseado na pressuposição de que para cada aspecto sensorial do observador há um correspondente evento fisiológico. De acordo com esta abordagem, a ta-

refa principal do pesquisador da percepção é isolar estes mecanismos fisiológicos subjacentes. A busca por unidades neurais específicas cuja atividade corresponda a experiências sensoriais específicas é comum a tais teorias.

Outra abordagem, a chamada *percepção direta*, envolve um conjunto de teorias que têm por base a premissa de que toda a informação necessária para a formação da percepção consciente está disponível nos estímulos que alcançam os receptores do indivíduo, ou em relações entre estes estímulos que são preditoras do que "está lá", no ambiente (COREN; WARD, 1989).

Outra abordagem, influenciada pelo desenvolvimento de sistemas de inteligência artificial e pela percepção direta, apresenta-se na forma de programas de computador que tentam simular a interpretação dos estímulos recebidos do ambiente, com o uso de vários estágios de análise. Por este motivo, esta abordagem ficou conhecida como *computacional* (COREN; WARD, 1989).

Uma abordagem mais antiga, mas ainda ativa, assume que a percepção do mundo é muito mais rica e mais acurada que o que se poderia esperar tendo por base apenas os estímulos vindos do ambiente. Assim, a estes estímulos seriam adicionadas experiências prévias, expectativas e assim por diante. Por envolver uma gama de fatores além dos puramente ambientais, esta abordagem é conhecida como*percepção inteligente*, também chamada de *teoria construtiva da percepção*, uma vez que a impressão final poderia envolver um número de diferentes fatores para construir a percepção resultante.

Em alguns meios, inclusive acadêmicos, discute-se ainda a *percepção extra-sensorial*, mas esta ainda não encontra amplo respaldo no meio científico (DAVIDOFF, 1983).

Segundo Coren e Ward (1989), cada uma das abordagens descritas acima parece ser válida para algumas partes do problema, mas irrelevante para outras. De todo modo, o rótulo aplicado é menos importante que o produto final em si, qual seja, a compreensão dos processos de percepção.

A.2.2 Fatores que influenciam a percepção

Como já se viu, pode-se definir a percepção como o processo pelo qual os indivíduos organizam e interpretam suas impressões sensoriais, com a finalidade de prover sentido ao ambiente que os rodeia. Viu-se, também, que esta percepção pode ser substancialmente distinta da realidade objetiva. Assim, o comportamento do indivíduo baseia-se em sua percepção da realidade e não na realidade em si: *"o mundo como é percebido é o mundo importante para o comportamento"* (ROBBINS, 2002, p. 46).

Uma série de fatores atuam para moldar e, às vezes, distorcer, a percepção. Tais fatores podem estar no observador, no objeto ou alvo da percepção, ou no contexto ou situação em que a percepção ocorre.

O observador

Quando se observa um alvo e se tenta interpretar o que se está percebendo, esta interpretação é fortemente influenciada pelas características pessoais do observador. Necessidades insatisfeitas ou *motivações* estimulam os indivíduos e podem exercer uma forte influência sobre a sua percepção. Do mesmo modo, *interesses* e *experiências passadas* também direcionam o enfoque do indivíduo, podendo, ainda, em contrapartida, anular o interesse por algum objeto (ROBBINS, 2002).

Por outro lado, objetos ou eventos que nunca foram antes experimentados são mais perceptíveis que aqueles já conhecidos, e por fim, as *expectativas* podem também distorcer a percepção, fazendo com que se veja aquilo que se espera ver; isto faz, por exemplo, com que alguém que espera que todos os políticos sejam corruptos, mesmo que não sejam, os veja daquela forma...

Estes conceitos individuais interiores, e mesmo anteriores ao momento em que a percepção se dá (pré-conceitos, na verdadeira acepção deste termo), causam impacto direto sobre a cognição, moldando-a e trazendo diferenças sensíveis sobre a "visão de mundo" dos diferentes indivíduos, mesmo que estes se postem diante de um mesmo fato, e são uma das fontes de discussão das teorias do conhecimento, conforme se vê no Capítulo 3.

O objeto

As características do objeto, ou alvo, que está sendo observado também podem afetar a percepção. Pessoas expansivas, por exemplo, costumam chamar mais a atenção do que as pessoas quietas. Como os alvos não são observados isoladamente e deslocados de todo o contexto, a sua relação com o cenário influencia a percepção, indicando a tendência de se agrupar coisas próximas ou parecidas.

O que se percebe irá depender, então, de como se separa o objeto de seu cenário geral. Exemplos clássicos e bastante claros disto são as imagens desenhadas pelo artista Maurits Cornelius Escher (ESCHER, 2002), como a reproduzida na Figura 11.

Objetos próximos uns dos outros tendem a ser percebidos em conjunto, seja esta proximidade física ou temporal. Isto ocorre com pessoas, objetos inanimados ou eventos - quanto maior a semelhança, maior a probabilidade de serem percebidos como um grupo.
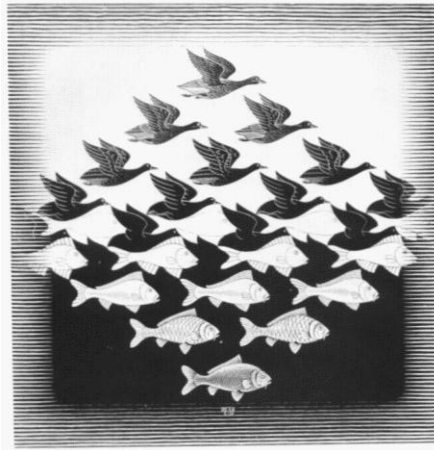
Figura 11: Escher, Litogravura. Fonte: Escher (2002).

O contexto

O contexto (ou situação) dentro do qual se percebe o objeto é igualmente importante, uma vez que os elementos que fazem parte do ambiente influenciam a percepção. Pode-se não se reparar numa determinada jovem de biquíni numa praia, num final de semana. Contudo, se ela usar os mesmos trajes numa cerimônia religiosa, com certeza chamará muito mais a atenção dos presentes. Mantidos o observador e o alvo, a mudança do contexto operou uma modificação radical na percepção. Além disso, fatores situacionais e ambientais, como a localização, a temperatura e a iluminação também influenciam na atenção que se dedica ao objeto.

Esquematicamente, a Figura 12 representa os fatores que influenciam a percepção.

Deste modo, o contexto é caracterizado pelas dimensões espaço-temporal e pragmática, ou seja, pelo arcabouço de acontecimentos que se observam durante o fenômeno que é percebido.

O passo seguinte à percepção é a tomada de decisões por parte dos indivíduos. No tocante à segurança da informação, estas são questões extremamente pertinentes: antes que se incorra nos gastos da adoção de políticas de segurança, convém avaliar se os usuários estariam propensos a segui-las. Até que ponto as pessoas estão dispostas a trocar a comodidade com a qual usualmente utilizam os seus sistemas de informação pelo desconforto causado pela implementação de medidas de segurança? Qual o grau de aceitação em trocar o comportamento corriqueiro por obediência (ou subserviência) a normas e padrões e mesmo sujeitar-se a invasão de privacidade (vide as iniciativas que se seguiram ao 11 de setembro) em contextos organizacionais e político-sociais? A mera alegação do aumento da segurança é suficiente para obter a aceitação dos usuários (e cidadãos), ou deve-se acrescentar demonstrações concretas de progressos tangíveis a fim de assegurar-se a cooperação? Qual o nível exigido de comprometimento da
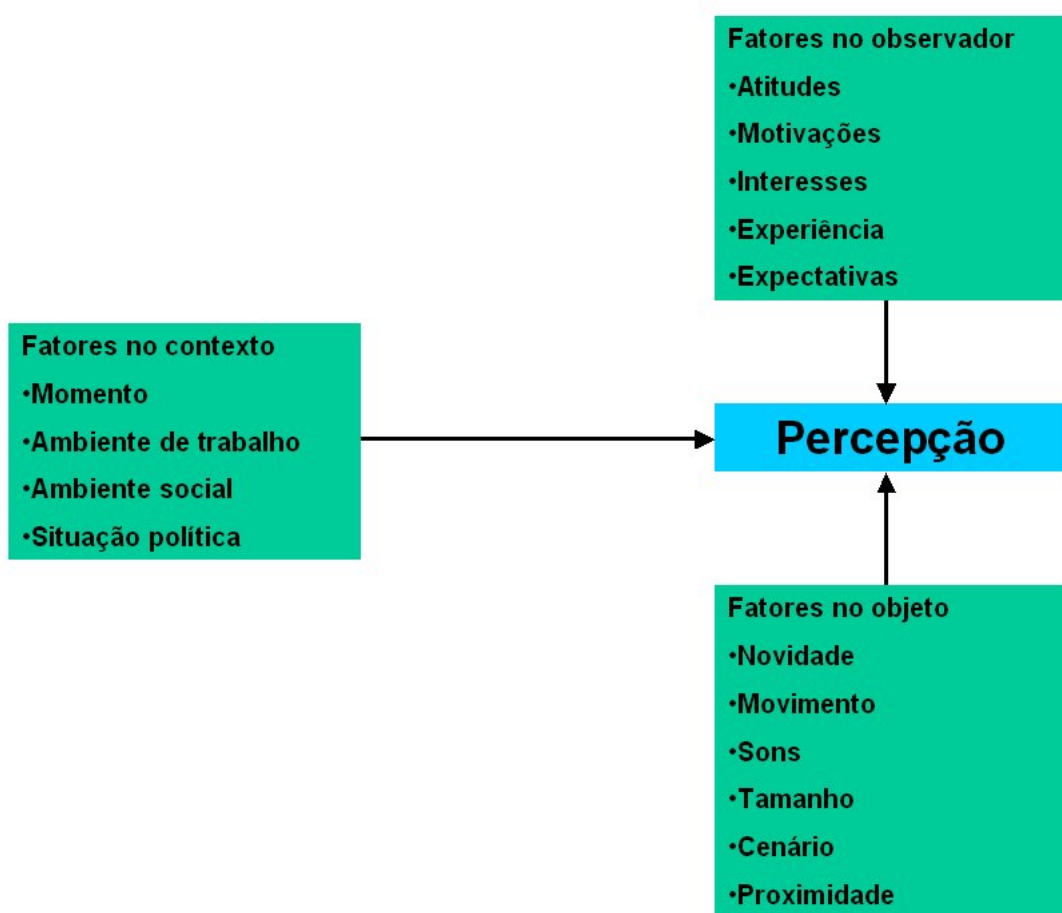
Figura 12: Fatores que influenciam a percepção [adaptada de Robbins (2002)].

organização em relação às políticas de segurança?

Estas questões, bem como os mecanismos psicológicos pelos quais um indivíduo estabelece suas escolhas e os conceitos éticos envolvidos na segurança da informação, serão descritos nas seções seguintes.

A.3 Aspectos éticos da segurança da informação

As primeiras discussões sobre a ética são atribuídas a Sócrates, que indagava aos cidadãos atenienses o que eles consideravam ser, em sua essência, atributos como coragem, justiça e piedade. Ao obter a resposta (usualmente, "são virtudes"), indagava novamente: "e o que é a virtude ?", e assim sucessivamente, até colocá-los em confronto com o que consideravam ser verdades arraigadas, questionando, assim, os usos e costumes de seus concidadãos.

É justamente a palavra "costume", que se diz, em grego, *ethos*, de onde vem o termo ética, e, em latim, *mores*, de onde vem moral. Porém, existe ainda o termo *ethos*, que significa caráter, índole natural, temperamento. Neste segundo sentido, refere-se ao senso moral e à consciência ética individuais. Aristóteles, por sua vez, acrescentou à consciência moral o aspecto da deliberação e da decisão ou escolha. Deste modo, a vontade guiada pela razão torna-se elemento fundamental da vida ética (CHAUI, 1999, p. 340-341).

Estes conceitos são apresentados aqui devido à acalentada discussão sobre a racionalidade de uma ética voltada ao uso de recursos informacionais e, de modo mais limitado, voltada ao uso de recursos computacionais, em uma era onde conceitos como privacidade e individualidade assumem novas feições, como se salienta, por exemplo, em Floridi (1999). Paradoxalmente, louvam-se, no mundo digital, ações de caráter coletivo, voltadas à disponibilização em esfera comunitária de recursos e fontes de informação, enquanto, de outro lado, a sociedade preserva como valores (e virtudes) a autonomia pessoal e a individualidade (THOMAS, 2002). Discute-se a expansão da chamada "autonomia moral" (WALDRON, 2002), onde o indivíduo se coloca frente ao grupo ao qual pertence, não mais perseguindo fins meramente individuais, mas voltados ao bem da coletividade e, como sugere Schmidt (2001), em harmonia com a natureza, e apresentam-se novos conceitos de "privacidade" (VOLKMAN, 2003) e "pluralismo moral"(NIEUWENBURG, 2004), destinados a acomodar os valores clássicos à realidade pós-moderna e à patente *desindividualização*, já comentada no Capítulo 4.

Especificamente no que diz respeito à segurança da informação, têm sido realizados estudos voltadas à apresentação de regras de conduta como preceitos éticos, constituindo requisito para a formulação de normas e controles para a implementação da segurança em sistemas. Leiwo e Heikkuri (1998), por exemplo, apresentam uma destas abordagens, onde uma conceitualização bastante pragmática da ética de grupos (por um lado *hackers* e pelo outro os profissionais da segurança da informação), é utilizada para a caracterização de seus comportamentos e para a obtenção de uma *lingua franca* na comunidade computacional, fundando-se um novo "contrato social" voltado às atividades digitais. Os próprios autores do trabalho reconhecem as imensas dificuldades de tal empreitada.

Outro aspecto a ser salientado diz respeito ao uso ético, ou seja, racional e moralmente aceitável, da tecnologia da informação, e, por extensão, da própria informação de que se dispõe ao à qual se realiza algum acesso. A este respeito, o estudo realizado por Phukan e Dhillon (2000) junto a 58 pequenas e médias empresas nos Estados Unidos mostra que questões como pirataria e uso ilegal de softwares permeiam o mundo corporativo, mesmo em organizações de porte no qual, teoricamente, o custo de legalizar-se os produtos utilizados seria menor (apenas

27,6% dos respondentes alegaram possuir cópias licenciadas dos softwares em uso em suas empresas). Por sua vez, Trompeter e Eloff (2001) apresentam um framework para a implementação de controles sócio-éticos na segurança da informação, baseados no respeito aos preceitos legais, enquanto Vroom e von Solms (2004) apontam para as dificuldades inerentes à auditoria das práticas adotadas pelos usuários. O estudo de Morahan-Martin e Schumacher (2000) mostra o uso "patológico" da internet entre estudantes universitários, uma das principais fontes de ataques a outras instituições.

Fala-se também em ética no mundo digital ao confrontar-se a atuação dos usuários e grupos que propugnam a livre utilização de recursos como obras científicas e artísticas às grandes corporações, principalmente de mídia, que procuram, sob a alegação de preservar seus investimentos, alternativas tecnológicas e legais (vide a seção 5.8) que impeçam ou diminuam a ação daqueles que, em alguns casos, apregoam a "desobediência civil digital" (LITMAN, 2003). Naturalmente, cada lado afirma ser "anti-ética" a atuação do oponente, enquanto outros, como Introna (2002) afirmam ainda ser impossível uma convivência racional baseada nos critérios e códigos estabelecidos na era da informação, requerendo uma nova ordem baseada na mediação face a face (e não em parâmetros comerciais ou tecnológicos) dos conflitos.

Embse, Desai e Desai (2004), em seu estudo sobre a aplicação de crenças, códigos e políticas no ambiente organizacional, apontam que para se concretizar a adoção de valores éticos é necessária a conjugação de uma abordagem abrangente, que contemple considerações estratégicas como performance, lucratividade e requisitos de qualidade, com vistas ao equilíbrio entre as normas propostas e a prática adotada, principalmente no nível operacional.

No ambiente organizacional, é fundamental o estabelecimento de confiança entre o usuário e a organização, caso se pretenda que aquele siga aos preceitos propostos por esta última (DUNN, 2000). A ética organizacional deve ser clara, concisa e livre de ambigüidades para que possa ser absorvida pelo indivíduo como um código de conduta que ele siga com um sentimento fundamental à sua situação como aliado: o prazer de agir de modo moral e reconhecidamente aceitável.

A.4 Cultura e comprometimento organizacionais voltados à segurança da informação

Cultura, como afirma Williams (apud VANDENBERGHE, 2003), é "uma das duas ou três palavras mais complicadas da língua". Vandenberghe (2003) segue apontando três significados distintos para o termo, um filosófico, um antropológico e um último associado ao senso comum.

No sentido mais amplo, cultura opõe-se a natureza, e assim representa tudo o que é criado pelo homem e é transmitido ou reproduzido por meio do convívio social - sem o homem não haveria cultura, mas sem cultura o homem também não subsistiria. O sentido seguinte avança do singular para o plural: “culturas” são expressões simbólicas de uma coletividade e são o que diferenciam esta coletividade das demais, por exemplo, as culturas egípcia, inca, babilônica ou européia. Por fim, cultura pode representar, dentro de cada uma daquelas culturas, um subsistema social, que difere dos demais subsistemas por características econômicas, políticas e jurídicas, e que por sua vez é internamente determinado por diferentes campos e subcampos de produção cultural e artística.

Em termos organizacionais, diversas acepções são dadas ao termo cultura, via de regra associadas ao comportamento, entendido como a manifestação da cultura, e vários intrumentos têm sido desenvolvidos para a aferição da cultura organizacional no que diz respeito a diversos temas (FERREIRA et al., 2002). No presente trabalho, pretende-se construir um instrumento capaz de avaliar as práticas da organização voltadas à segurança da informação e que esteja apto a responder as seguintes questões: até que ponto as normas e práticas adotadas no ambiente organizacional podem de fato orientar os usuários e serem absorvidas por eles como códigos de conduta? Em outras palavras, quanto o comportamento organizacional é capaz de efetivamente influenciar o comportamento individual? E ainda, em que grau se dá a relação inversa, ou seja, o comportamento adotado pelos usuários é capaz de ditar o comportamento organizacional?
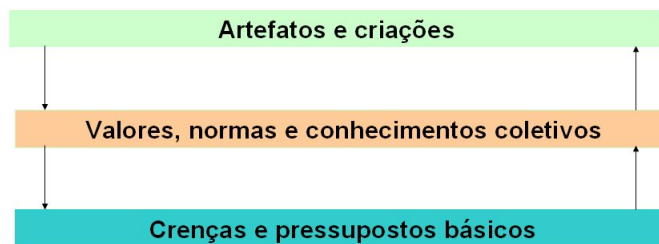
Figura 13: Cultura organizacional na visão de Schein (apud VON SOLMS; VON SOLMS, 2004).

Para Schein (apud VON SOLMS; VON SOLMS, 2004), conforme a Figura 13, a cultura organizacional se apóia sobre pressupostos e crenças básicas que influenciam os membros dos grupos, seus pensamentos e sentimentos, sendo assim expressa na forma de valores, norma e conhecimento coletivos, os quais, por meio das normas e regras expressas ou mesmo implícitas, afetam o comportamento dos indivíduos e resultam em ações, criações e artefatos. Deste modo, a modificação desejada no comportamento deve ser proposta por meio das regras e normas a serem seguidas.

Diversos estudos, tais como o de Spurling (1995), apontam para a necessidade de incrementar-

se a consciência quanto à segurança da informação nos limites da organização. Diversas abordagens têm sido propostas, sendo que algumas destas são discutidas a seguir.

A "segurança da informação comportamental" aborda as ações humanas que influenciam os aspectos de confidencialidade, disponibilidade e integridade dos sistemas de informação (STANTON et al., 2003). Os autores realizaram junto a organizações nos Estados Unidos dois estudos baseado no comprometimento organizacional, uma variável atitudinal bastante utilizada em estudos em ambientes organizacionais, e que está associada ao grau em que o indivíduo aceita e realiza as práticas prescritas no referido ambiente. Um dos resultados obtidos é que o comprometimento organizacional está positivamente relacionado à adoção de práticas voltadas à segurança sem, contudo, esclarecer os motivos para tal associação. Outro resultado, contrário ao senso comum, indica que usuários com alto grau de comprometimento organizacional têm menor índice de aceitação de políticas de uso aceitável (políticas que descrevem o uso consideradas adequado de recursos computacionais disponibilizados pela organização). Os autores apenas lançam conjeturas sobre a razão de tal comportamento, entre elas, a de que indivíduos com alto grau de identificação com a organização se sintam em tal grau de liberdade que terminem por repudiar as normas que pretendam ditar seus passos. De todo modo, fica claro que a compreensão do comportamento dos usuários frente às práticas de segurança é um elemento essencial às abordagens puramente tecnológicas. Em outro estudo posterior, Stanton et al. (2005) apontam a formação de padrões de comportamento (por eles intituladas taxonomias) relacionadas a diferentes práticas relacionadas ao uso e construção de senhas de acesso a sistemas, e reforçam a necessidade de treinamento e capacitação como medidas destinadas a diminuir a incidência de práticas contrárias aos preceitos de segurança.

Schlienger e Teufel (2003) apresentam um estado sobre a cultura da segurança da informação, introduzida como participante da cultura organizacional, a qual é expressa pelos valores, normas e conhecimento da organização. A cultura da segurança agrega a análise das políticas de segurança e a obtenção, junto aos usuários e aos gestores da informação e da segurança, dos valores reais adotados no ambiente organizacional a fim de orientá-los e utilizá-los como subsídios às práticas da segurança, buscando, complementarmente, a inserção de tais práticas no conjunto dos valores organizacionais.

Lee e Lee (2002), por sua vez, observando que o volume de abusos cometidos com o uso de computadores não diminui ao longo do tempo (vide a seção 4.3), mesmo com a adoção de práticas e políticas, sugerem a adoção de um modelo abrangendo as teorias da criminologia social com vistas à diminuição de tais abusos.

Por fim, von Solms e von Solms (2004) alertam para a necessidade de educação dos usuários

voltada às políticas como forma de apoiar sua implementação e utilização e para formação da cultura organizacional voltada à segurança. Por sinal, a educação dos usuários já tem sido enfatizada em outras análises, como, por exemplo, no tocante ao uso de senhas de acesso a sistemas (SASSE; BROSTOFF; WEIRICH, 2001; STANTON et al., 2005) e outras formas de abuso dos recursos tecnológicos (STRAUB, 1990; THOMSON, 2001).

A.4.1 O "elo mais fraco"

Já foi salientada a afirmação (vide Capítulo 4), comum no âmbito dos profissionais de segurança da informação, de que os usuários representam o elo mais fraco da "corrente" formada pela tríade tecnologia, pessoas e processos. Porém, esta afirmação é francamente discutível.

No contexto do levantamento de requisitos para a implementação de sistemas de informação, por exemplo, há ocorrências de falhas de implementação decorrentes do subdimensionamento das relações de poder existentes entre os diversos usuários (DHILLON, 2004). Por outro lado, o papel essencial representado pelos gestores da segurança torna-os tão ou mais vulneráveis que os usuários ditos "comuns", fazendo com que sua escolha e treinamento se tornem ações essenciais e impactantes sobre todo o processo de segurança (RHODEN, 2002; GUZMAN; KAARST-BROWN, 2004). Por sua vez, todos os equipamentos utilizados no fluxo das informações consideradas sensíveis devem, necessariamente, ser objeto de atenção especial, e não somente as estações utilizadas pelos usuários finais (ARCE, 2003b).

A.4.2 Comportamento, aceitacão e uso da tecnologia

Por trás da utilização dos recursos tecnológicos no âmbito dos sistemas de informação em ambientes organizacionas, estão os processos de decisão que levaram à escolha e à adoção de tais recursos. Estas escolhas, que aparentemente são feitas de modo racional e objetivo, podem ser realizadas, na verdade, com base em intuições e rituais que fogem completamente à alçada da tomada racional de decisões (TINGLING; PARENT, 2004), o que irá, certamente, gerar conseqüências sobre todo o ciclo de vida de tais sistemas. Konana e Balasubramanian (2005), por exemplo, propõem um modelo com bases sócio-econômico-políticas, e não apenas econômicas ou mercadológicas, para a escolha e adoção de recursos tecnológicos em organizações, enquanto Legris, Ingham e Collerette (2003) apresentam um modelo de aceitação de TI, com bases em critérios subjetivos.

Outro aspecto de grande impacto sobre o uso de sistemas de informação e conseqüentemente sobre a adoção de práticas de de utilização destes sistemas, como as políticas de segu-

rança da informação, é a resistência a mudanças. Vann (2004) apresenta um estudo sobre tal resistência a mudanças em projetos de TI na área governamental, advogando a adoção de uma linguagem ("gramática") capaz de dimimuir o impacto da apresentação dos projetos. Ashforth e Kreiner (2002) apontam sugestões para a normalização de emoções no ambiente organizacional, ou seja, para a adoção mais rápida de práticas ritualísticas advindas de normas recentemente introduzidas - quanto mais rapidamente a prática se torna um ritual, mais facilmente a norma é obedecida, evitando assim o individualismo e os comportamentos aversivos às práticas prescritas como adequadas, comportamentos estes que são o objeto do estudo de Preece, Nonnecke e Andrews (2004) em comunidades digitais.

Qualquer que seja o modelo adotado para a adoção das normas, e mais especificamente, das políticas de segurança da informação, a sua adoção sempre estará sujeita ao crivo dos indivíduos dos quais se espera o seu cumprimento. A regulação coletiva é dependente da auto-regulação (KAROLY, 1993), e, por outro lado, alimenta-se dela para a sua existência. Assim sendo, o comportamento coletivo é dependente e ao mesmo determinante do comportamento indivivual, motivo pelo qual este trabalho propõe a análise acurada da dinâmica do indivíduo, no contexto organizacional, no tocante à segurança da informação, fechando o ciclo entre a interação social (vide Capítulo 6) e a implementação efetiva de políticas de segurança da informação.

A.5 Processos psicológicos associados à tomada de decisão

A economia comportamental (*behavioural economics*), que levou posteriormente à teoria da escolha (HEAP et al., 1992), amplamente fundamentada sobre a a psicologia e as ciências cognitivas, associa-se à teoria dos jogos clássica para analisar a tomada de decisão, no que cunhou uma expressão peculiar: a "psicologia da preferência". Alguns resultados contrariam o senso comum sobre os conceitos objetivos e subjetivos sobre a tomada de decisões; por exemplo, a ameaça de perda tem impacto maior sobre uma decisão do que a possibilidade de um ganho equivalente. Dois tipos de comportamento são identificados: o de aversão ao risco (*risk aversion*), caracterizado se um retorno garantido é preferido em relação a um jogo cuja expectativa de retorno é equivalente ou maior, e o de busca do risco (*risk seeking*), caracterizado se o retorno garantido é rejeitado em favor de um jogo com expectativa de retorno equivalente ou menor. Os estudos psicológicos indicam que a preferência entre ganhos é de aversão ao risco e que a preferência entre perdas é de busca do risco. De qualquer modo, é fundamental no processo de decisão o efeito de enquadramento (*framing effect*), ou seja, o contexto no qual se dá a tomada de decisão, e modo pelo qual este contexto é percebido pelos indivíduos (KAHNEMAN; TVERSKY, 1982; VRANAS, 2000). Em um texto posterior, Kahneman (2003) avança

ainda sobre os aspectos de intuição e julgamento posteriores à percepção. Outro aspecto relevante é abordado no estudo de Feldman, Miyamoto e Loftus (1999): seria o fato de não agir diante de determinada situação mais pesaroso que agir e não obter o retorno desejado? Muitos fatores pesam sobre a resposta a esta questão. O motivo dela ser abordada no contexto da segurança da informação é devida à expectativa frente ao comportamento dos usuários: eles irão ou não adotar as condutas ditadas pelas políticas de segurança da informação? Em cada caso, afirmativo ou negativo, qual o grau de satisfação ou insatisfação obtido? A este respeito, também o estudo de Idson, Liberman e Higgins (2002) trata da diferenciação entre perdas e ganhos diante de decisões envolvendo riscos, tema aprofundado por autores como Munro e Sugden (2003), Kleiter et al. (1997), Fontana e Gerrard (2004), Yang e Qiu (2005), Tamura (2005) e Ratner e Herbst (2005) e, nos ambientes organizacionais, por Kwak e LaPlace (2005).

A.6 A construção do instrumento de percepção positiva da segurança da informação

Uma vez definido o sistema que será objeto de estudo do instrumento, passa-se à qualificação do atributo ou dos atributos de interesse, a fim de delimitar-se os aspectos específicos para os quais se deseja construir o instrumento de medida (PASQUALI, 1999).

A.6.1 As propriedades do sistema psicológico

A propriedade da percepção que se deseja analisar com o instrumento construído neste trabalho é a **percepção positiva a respeito da segurança da informação**. Ou seja, deseja-se saber qual o grau de aderência dos respondentes do instrumento, que serão usuários de sistemas de informação em instituições públicas e privadas, servidores ou empregados de tais instituições, a práticas voltadas para a segurança da informação. Noutras palavras, deseja-se aferir o grau com que o indivíduo percebe (compreende) o tema da segurança da informação como uma característica essencial ao seu trabalho.

Infelizmente, não existe uma teoria construída e consolidada sobre esta propriedade, especificamente. Sobre a percepção, como se viu, existem as mais diversas teorias. Contudo, a respeito da propriedade específica que é a percepção da segurança da informação, não existem construtos teóricos elaborados. Assim sendo, passa-se à enumeração dos construtos que se considera relevantes nesta pesquisa, em direção à elaboração de uma mini-teoria que, espera-se, venha a ser corroborada pelos dados empíricos (PASQUALI, 1999, p. 44).

A.6.2 Definições do construto

Definição constitutiva

O construto "percepção positiva a respeito da segurança da informação", para os efeitos a que se propõe este trabalho, é definido como a *capacidade de realizar tarefas que estejam voltadas para a implementação da segurança da informação, de modo autônomo e sem (ou com poucas) resistências*.

Definição operacional

Por pleonástico que possa parecer, a definição operacional do construto "percepção positiva a respeito da segurança da informação" é *realizar tarefas que estejam voltadas para a implementação da segurança da informação, de modo autônomo e sem (ou com poucas) resistências*.

As atividades, aqui indicadas como categorias comportamentais, obtidas da literatura de segurança da informação [(ABNT, 2002),(WOOD, 2002b), (BOSWORTH; KABAY, 2002)] e que são identificadas pelo autor com semelhante comportamento, devendo originar a seguir os itens do instrumento e sendo já descritas em tais termos, são as seguintes:

1. realizar cópia periódica (*backup*) dos dados sob a sua guarda;
2. substituir periodicamente as senhas de acesso aos sistemas de informação de que faz uso;
3. utilizar senhas seguras, com variação de caracteres, a fim de evitar ou pelo menos dificultar sua descoberta;
4. realizar periodicamente a atualização dos sistemas de proteção contra vírus em seu equipamento;
5. configurar os sistemas de proteção contra vírus para realizar varredura automática;
6. verificar a origem de arquivos anexados em e-mails (mensagens de correio eletrônico) antes de abri-los;
7. encerrar adequadamente a conexão a sistemas de informação;
8. bloquear o acesso ao computador, por meio de senha, ou desligá-lo antes de se ausentar por períodos prolongados;
9. verificar a voltagem do computador antes de ligá-lo à rede elétrica;

10. utilizar filtros de linha ou *no-breaks* para a conexão à rede elétrica;
11. guardar documentos sigilosos em local seguro;
12. não ingerir líquidos ou alimentos próximo a computadores ou equipamentos eletrônicos sensíveis à sujeira ou umidade;
13. não permitir o compartilhamento de arquivos ou conjuntos de arquivos (pastas e diretórios), exceto sob estrito controle;
14. não instalar software de origem desconhecida ou incerta;
15. realizar a limpeza periódica do repositório de arquivos removidos (lixeira);
16. não digitar senhas ou outras informações sigilosos em equipamentos não confiáveis;
17. não expor equipamentos eletrônicos a condições de temperatura e umidade inadequadas (fora das especificações do fabricante);
18. instalar software de controle de acesso (*firewall*) no computador de uso pessoal no ambiente de trabalho;
19. ler relatórios e notícias relacionados aos eventos da segurança da informação;
20. manter-se atualizado sobre a existência de vírus, cavalos de tróia (porções de código que se instalam em computadores e aparentam atividades distintas daquelas danosas que realmente realizam) e outras formas de programas e códigos maliciosos;

Construção dos itens

Os itens constantes do instrumento procuram adequar-se aos critérios definidos por (PASQUALI, 1999), a saber:

1. Critério comportamental: os itens expressam comportamentos, e não abstrações;
2. Critério de desejabilidade ou preferência: os itens cobrem atitudes, medidas como comportamentos desejáveis;
3. Critério da simplicidade: cada item expressa uma única idéia;
4. Critério da clareza: pretende-se que os itens sejam inteligíveis para todos os estratos de respondentes (usuários de sistemas de informações, servidores de instituições públicas e/ou privadas);

5. Critério da relevância: a frase contida nos item é consistente com o atributo que se deseja medir (percepção positiva a respeito da segurança da informação);

6. Critério da precisão: os itens possuem posições definidas no contínuo do atributo, sendo distintos dos demais itens; esta asserção deve ser verificada com a coleta dos dados empíricos;

7. Critério da variedade: deve ocorrer variação da linguagem de um item para outro, evitando a monotonia do respondente, e deve também ocorrer variação na escala de preferências, indicando metade dos itens em termos favoráveis e metade em termos desfavoráveis, para evitar erros de resposta estereotipada;

8. Critério da modalidade: evita-se a formulação de itens com linguagem extremada, sem o uso de expressões como “o melhor”, “o pior”, e congêneres;

9. Critério da tipicidade: as frases são formuladas com expressões condizentes com o atributo;

10. Critério da credibilidade: os itens não devem ser formulados de modo a parecerem ridículos, despropositados ou infantis;

11. Critério da amplitude: o conjunto de itens procura cobrir toda a magnitude do construto pesquisado, procurando identificar e discriminar entre os sujeitos que possuem diferentes traços de comportamento com relação ao construto;

12. Critério do equilíbrio: procura-se elaborar itens fáceis, médios e difíceis, cobrindo de modo proporcional todos os segmentos do contínuo.

Quanto à quantidade de itens, propõe-se a elaboração de um número igual a 20 seguindo a regra do bom senso expressa por Pasquali (1999, p. 51), o que resulta em um item para cada uma das atividades listadas anteriormente.

O instrumento construído está no Apêndice B.

APÊNDICE B – Instrumento de captura da percepção da segurança da informação

Caro (a) leitor (a),

O questionário seguinte é componente de uma pesquisa feita em uma tese de doutorado voltada à segurança da informação. Não é necessário se identificar.

Responda às questões, assinalando a opção correspondente ao comportamento que você adota diante de cada uma das situações apresentadas.

Muito obrigado por sua atenção.

1.Realizo cópia de segurança (*backup*) dos dados da instituição em que trabalho quese encontram sob a minha guarda.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

2.Ao atualizar as senhas de acesso, utilizo senhas distintas das anteriores.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

3.Utilizo senhas fracas (compostas por nomes ou iniciais de pessoas conhecidas, datas de eventos pessoais, seqüências de letras ou números evidentes).

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

4.Leio as ofertas de negócios e oportunidades que me são enviadas por correio eletrônico sem a minha solicitação.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

5. Ao tratar de assuntos pessoais, utilizo conta de correio eletrônico distinta da organizacional.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

6. Executo arquivos anexados recebidos por correio eletrônico.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

7. Após utilizar sistemas de informação, eu encerro a sessão (faço *logoff*).

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

8. Ao ligar um novo computador ou outro equipamento à rede elétrica, primeiro verifico a voltagem de ambos (equipamento e rede).

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

9. Utilizo filtros de linha ou *no-breaks* para a ligação de computadores e periféricos à rede elétrica.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

10. Ao me ausentar de meu local de trabalho, encerro a sessão aberta no computador (faço *logoff*), bloqueio a sessão com uso de senha, ou o desligo.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

11. Guardo documentos de caráter sigiloso em local seguro.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

12. Consumo alimentos líquidos ou sólidos ao trabalhar diante de computadores ou periféricos.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

13. Nos computadores em que possuo tais direitos, permito o compartilhamento de arquivos ou conjuntos de arquivos (pastas e diretórios).

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

14. Nos computadores em que possuo tais direitos, instalo programas baixados da internet.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

15. Leio relatórios e notícias relacionados aos eventos da segurança da informação.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

16.Faço a limpeza do repositório de arquivos removidos (lixeira) de meu computador.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

17.Digito senhas para consulta a sistemas e correio eletrônico em computadores, bastando que estejam à minha disposição.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

18.Verifico as condições de temperatura e umidade às quais estão expostos computadores e periféricos.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

19.Procuro conhecer as normas da instituição a respeito do uso de computadores e sistemas computacionais.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

20.Eu me atualizo sobre a existência de vírus, cavalos de tróia (programas que se instalam em computadores e aparentam atividades distintas daquelas danosas que realmente realizam) e outras formas de programas e códigos maliciosos.

Sempre ☐ Freqüentemente ☐ Às vezes ☐ Raramente ☐ Nunca ☐

Por gentileza, forneça agora alguns dados para aumentar ainda mais a utilidade deste questionário. Estes dados não serão utilizados para a identificação de qualquer respondente.

21. Você é: _____ Homem _____ Mulher

22. Sua idade é: _____ anos

23. Você trabalha nesta instituição:
_____Há menos de um ano
_____Um ano ou mais, mas menos que cinco anos
_____Cinco anos ou mais, mas menos que dez anos
_____Há dez anos ou mais

24. Seu grau de instrução é:
_____Nível fundamental incompleto
_____Nível fundamental completo
_____Nível médio incompleto
_____Nível médio completo
_____Nível superior incompleto
_____Nível superior completo
_____Especialização
_____Mestrado ou doutorado

Sinta-se à vontade para fazer quaisquer sugestões e apresentar eventuais comentários ao questionário ou aos temas que ele aborda:

____

____

____

____

____

____

APÊNDICE C – Lógica e Segurança da informação

C.1 A formalização da segurança em sistemas de informação

A utilização de modelos lógicos formais está intrinsecamente ligada aos sistemas de informação: assim como o conhecimento pode ser representado por meio de mecanismos lógicos, a própria configuração dos computadores baseados na máquina de Turing é diretamente mapeada por sistemas lógicos (portas), bem como os passos para a programação destes computadores (algoritmos). Além disso, a Inteligência Artificial, integrando a ciência da computação e as ciências cognitivas, faz uso de formalismos lógicos para o desenvolvimento de sistemas especialistas e outros modelos de mimetização do raciocínio, como agentes inteligentes.

Uma das principais utilizações dos sistemas formais baseados na lógica, no que diz respeito aos sistemas de informação, apresenta-se no desenvolvimento de softwares, com o uso de mecanismos voltados ao levantamento e à validação de requisitos. Esta utilização, porém, não é amplamente disseminada, uma vez que ferramentas e metodologias estruturadas ou orientadas a objetos, como os padrões propostos pela ISO e o Capability Maturity Model - CMM, são as preferidas pelas equipes de desenvolvimento (ASHRAFI, 2003).

Especificamente no que diz respeito à segurança da informação, o uso de modelos lógicos é mais usual na formalização e validação de protocolos, notadamente aqueles voltados à verificação e autenticação de usuários, processos e sistemas (ABADI; BLANCHET, 2005; ACCORSI; BASIN; VIGANÒ, 2003; RAMANUJAM; SURESH, 2003; LOWE, 1998). Nestes casos, interesse especial é devotado ao fluxo da informação. Para este fim, modalidades da lógica têm sido particularmente desenvolvidas, como as lógicas de alternância temporal (ALUR; HENZINGER; KUPFERMAN, 1997; van der Hoek; WOOLDRIDGE, 2003; KREMER; RASKIN, 2001).

Além dos formalismos lógicos para a segurança, outras modalidades também foram apresentadas com o mesmo fim: parametrizar os requisitos do fluxo da informação com vistas à segurança computacional (MCLEAN, 1988, 1990a, 1990b), utilizar-se formalismos gráficos,

como redes de Petri, utilizadas em modelos de segregação de papéis(ELSAS; VRIES; RIET, 1998) e análise de incidentes (STEPHENSON, 2004), prover o desenvolvimento de linguagens para a modelagem de restrições de acesso (DAMIANOU et al., 2001), e implementar-se camadas de software como mediadoras do acesso a bases de dados (DAWSON; QIAN; SAMARATI, 2000). Além destas abordagens, também a teoria da eleição ou da escolha social já foi proposta como estratégia para seleção de comportamentos coletivos entre usuários de sistemas de informação em redes ponto a ponto (SERJANTOV; ANDERSON, 2004).

É necessário acrescentar que estes modelos não têm por objetivo eliminar totalmente eventuais vulnerabilidades nos protocolos ou nos sistemas que os utilizam, mas sim visam a minorá-las, uma vez que detectar todos os fluxos e pontos de acesso ou processamento inseguros em um sistema, e somente estes, é um problema indecidível (DENNING, 1982 apud MCLEAN, 1988), ou seja, não existe um algoritmo de complexidade temporal finita capaz de dizer se um determinado sistema computacional que faça uso de tais protocolos está totalmente isento de vulnerabilidades. Em outras palavras, do ponto de vista da segurança, todo sistema é intrinsicamente vulnerável.

De maneira geral, tem ocorrido uma integração entre a formalização do desenvolvimento de software e a formalização da segurança com base em seus requisitos (particularmente os aspectos de confidencialidade,integridade e disponibilidade), além da autenticação de usuários (HAMMONDS et al., 1995) e a verificação de componentes não mutáveis do sistema (BOSSI et al., 2004). De modo coerente, os métodos existentes para a implementação de projetos de segurança da informação no desenvolvimento de sistemas acompanham *pari passu* as ferramentas de desenvolvimento de sistemas (BASKERVILLE, 1993), mesmo as mais modernas (SIPONEN, 2005) - o que não impede a produção de softwares com vulnerabilidades decorrentes de falhas flagrantes de desenvolvimento.

Metodologicamente, os modelos desenvolvidos neste âmbito têm se dividido entre as formas de controle de acesso relativas aos sistemas desenvolvidos, divididas em três grandes categorias: DAC (*discretionary access control*), onde o acesso dos usuários aos recursos é controlado conforme métricas voltadas ao negócio, MAC (*mandatory access control*), onde o acesso é codificado no próprio sistema, ou RBAC (*rule-based access control*), onde o acesso é dinamicante atribuído conforme o papel desempenhado pelo usuário junto ao sistema (LOPEZ; OPPLIGER; PERNUL, 2004; CHOU, 2004a; BELLETTINI; BERTINO; FERRARI, 2001; SANDHU et al., 1996; KAGAL; FININ; PENG, 2001; AHN; HONG; SHINC, 2002). Mais recentemente, com a disseminação de sistemas de ampla abrangência, principalmente a internet, procedeu-se à montagem de infra-estruturas de autenticação e autorização de usuários, com

o uso de recursos de assintaura e autenticação baseados em criptografia assimétrica, como o sistemas .NET da Microsoft (LOPEZ; OPPLIGER; PERNUL, 2004). Outra abordagem é a assim chamada “muralha chinesa” (BREWER; NASH, 1989; SOBEL; ALVES-FOSS, 1999; FOLEY, 1997; MEADOWS, 1990), onde diferentes perfis de acesso determinam os limites dentro dos quais se permite ou se limita o acesso à informação.

Como se observa, a grande maioria dos modelos de segurança discutidos neste âmbito limita-se, por um lado, aos aspectos do desenvolvimento de software e, por outro, ao fluxo da informação envolvido na dinâmica dos sistemas, com o desenvolvimento de protocolos e ferramentas de propósito geral, mas que, na verdade, abordam exclusivamente os aspectos da tecnologia envolvida na concepção, projeto e desenvolvimento de softwares (num momento pré-existencial, ou seja, anterior à existência dos sistemas) ou no acesso aos recursos disponíveis (num momento pós-existencial, ou seja, já com os sistemas desenvolvidos e em funcionamento e quando o custo de atualizações e modificações se mostra excessivamente oneroso).

Este panorama complica-se ainda mais quando se percebe que o objetivo das políticas pode ser distinto, variando conforme a missão ou visão organizacionais, ou de acordo com o nicho de negócios. No âmbito militar, por exemplo, historicamente, a principal meta das políticas desenvolvidas tem sido a confidencialidade, ao passo que nas organizações comerciais dá-se ênfase à integridade da informação - mas um requisito não exclui o outro. Comparações como a realizada por Clark e Wilson (1987) ilustram a complexidade advinda da necessidade de contemplar-se estes requisitos no bojo de uma mesma organização.

Muito pouco se tem desenvolvido sobre a formalização da segurança dos sistemas computacionais enquanto repositórios de informação e como fontes de conhecimento potencial, enfocando a dinâmica da interação dos usuários com o sistema e entre si. Mesmo textos de análise crítica de modelos de segurança (MCLEAN, 1997) ou de verificação dos padrões de segurança e confiabilidade apontam na direção de maiores requisitos tecnológicos, como a tolerância a falhas (MEADOWS; MCLEAN, 1998), como solução para o caos da segurança que se tem apresentado.

É conveniente salientar um dos principais motivos por que os modelos de formalização acima descritos são insuficientes para modelar a segurança da informação de modo abrangente: estes modelos se restringem ao domínio dos processos e componentes não humanos do sistema e, ao tratar os usuários, estes são apontados como componentes estanques, sem vontade própria ou com um comportamento sempre uniforme e determinístico - na verdade, em muitos casos a segurança é reportada como sendo computacional (*computer security*). Deste modo, é possível possuir-se um sistema de elevada aderência aos padrões de segurança estipulados por tais mo-

delos, mas que se vê burlado pelo comportamento incongruente (mas por vezes até previsível) de agentes humanos ou de outra natureza, os quais não foram adequadamente contemplados na elaboração do modelo.

Contrariamente, este trabalho preconiza a formalização de políticas de segurança da informação como um mecanismo de padronização de práticas voltadas não somente aos momentos de desenvolvimento ou de manutenção de sistemas, mas também ao comportamento esperado de usuários de todos os níveis e perfis frente a tais sistemas.

Alguns trabalhos que apresentam modelos para a formalização da segurança em sistemas de informação envolvem a conjunção dos formalismos da lógica com a teoria dos jogos, buscando modelar as interações envolvidas na tomada de decisões pelos usuários destes sistemas (ALFARO; GODEFROID; JAGADEESAN, 2004; LAMARCHE, 1995; BAILLOT; DANOS; EHRHARD, 1997). Também na especificação e na formalização de protocolos a teoria dos jogos tem sido usada (KREMER; RASKIN, 2002), assim como na análise da interação entre grupos (PARIKH; RAMANUJAM, 2003) e na montagem de modelos concernentes ao conhecimento do usuário sobre a informação contida no sistema (PARIKH; VÄÄNÄNEN, 2005). Em todos estes casos, a ação do usuário se dá sob parâmetros bem delimitados, considerando-se sua plena anuência quanto ao fluxo da informação e quanto aos processos envolvidos na execução do sistema.

Contudo, não se encontrou um modelo que agregue os formalismos da lógica, a estrutura analítica da teoria dos jogos e a verificação do comportamento dos usuários para a formalização de políticas de segurança da informação, como se propõe neste trabalho. A fim de elucidar os formalismos a serem usados, alguns dos termos usuais no meio da segurança da informação serão mantidos, enquanto outros serão apresentados sob nova roupagem e outros ainda, redefinidos ou introduzidos. Em cada um destes casos, será feita uma indicação ao leitor, para que ele possa elaborar comparações com outros trabalhos. Serão evitadas, tanto quanto possível, remissões à tecnologia empregada: no intuito de ser abrangente, o modelo deve ser independente da plataforma de implementação.

C.1.1 Classificação das lógicas modais

Entre as lógicas modais, destacam-se particularmente as seguintes:

- lógicas modais ônticas: são capazes de tratar sentenças do tipo "É necessário / possível / impossível que *p*", onde *p* representa um predicado lógico (um fato ou uma regra do mundo real);

- lógicas modais temporais: são capazes de tratar sentenças do tipo "É / será (sempre / em dado momento) verdade que p";
- lógicas modais deônticas: capazes de tratar sentenças como "É (obrigatório / permitido / proibido) que p";
- lógicas modais epistêmicas: são capazes de tratar sentenças como "x sabe que p.", onde x representa um ator (humano ou automatizado) do sistema em consideração;
- lógicas modais doxásticas: são capazes de tratar sentenças do tipo "x (acredita / pensa / considera) que p".

Eis o exemplo de uma sentença comum numa política de segurança da informação, extraído de Cholvy e Cuppens (1997):

"Qualquer agente no papel de Usuário tem permissão para ler qualquer arquivo público".

Esta frase pode ser traduzida conforme a seguinte sentença da lógica modal:

$$\forall f, \forall A, Arq(f) \wedge Publico(f) \wedge Papel(A, Usuario) \rightarrow \Diamond Ler(A, f) \quad (C.1)$$

Os termos e símbolos dispostos na Equação C.1 estão explicitados na Tabela 10.

Termo ou símbolo	Significado
$\forall x, q(x)$	quantificador universal (lê-se "para todo $x, q(x)$") - indica que q aplica-se a todas as ocorrências de x
$a \wedge b$	conjunção (lê-se "a e b") - é satisfeito (é verdadeiro) quando a e b são ambos satisfeitos
$p \rightarrow q$	conseqüência lógica (lê-se "p implica q") - indica que, uma vez satisfeito p, satisfaz-se q
$Arq(x)$	predicado lógico que é satisfeito se x é um arquivo
$Publico(x)$	predicado lógico que é satisfeito se x é público
$Papel(x,y)$	predicado lógico que é satisfeito se x desempenha o papel y
$\Diamond q$	operador modal de possibilidade (lê-se "é possível q")
$Ler(x,y)$	predicado lógico que é satisfeito se o argumento x lê o argumento y

Tabela 10: Termos e símbolos presentes na Equação C.1.

C.2 Lógicas modais e a formalização de políticas de segurança

A motivação da escolha, neste trabalho, de um modelo formal baseado na lógica para a especificação de políticas de segurança deve-se à ênfase que se pretende imprimir à verificação de tais políticas por meio de provas formais. Este processo se inicia pela representação das políticas numa linguagem formal, livre das ambigüidades das linguagens naturais e que permita a integração de todos os elementos envolvidos com os conceitos da segurança, por meio da validação do modelo construído. Proceder-se-á, assim, à formulação e à validação das políticas por meio dos mecanismos da lógica e à sua transposição para a linguagem natural, a fim de que sejam lidas, interpretadas, compreendidas e executadas pelos atores humanos.

Por seu turno, a escolha do formalismo das lógicas modais advém da sua capacidade de tratar modalidades do conhecimento (HUGHES; CRESSWEL, 1984, 1996) presentes em situações do dia a dia, capacidade esta ausente das lógicas de primeira ordem convencionais (EPSTEIN, 1990, 1994).

A utilização de lógicas modais se extende desde os modelos de formalização de protocolos e fluxos da informação, já citados, passando pela representação epistêmica de fluxo da informação em sistemas probabilísticos (SYVERSON; GRAY, 1995), a análise da inter-relação entre as lógicas epistêmicas e a ciência cognitiva (PIETARINEN, 2003) e a busca por uma semântica do conhecimento comum (LISMONT; MONGIN, 1995).

C.2.1 Uma lógica do conhecimento

Um dos principais trabalhos a utilizar-se de lógicas modais para a formalização da segurança foi o de Glasgow, MacEwen e Panangaden (1992), onde foram estabelecidas as modalidades de permissão (para políticas de confidencialidade) e de obrigação (para lógicas de integridade). A teoria resultante, denominada lógica de segurança (*Security Logic - SL*),pode ser então utilizada para especificar quando interagem os componentes tempo, conhecimento, obrigação e permissão. De fato, duas propriedades fundamentais da segurança são expressas usando-se SL:

1.um indivíduo [1] conhece apenas fatos para os quais tem a permissão de conhecer; e

2.se um indivíduo é obrigado a saber algo, eventualmente ele o saberá.

[1]Neste capítulo, por “indivíduo” ou “sujeito” designa-se o usuário de sistemas de informação, seja ele humano, um processo ou um outro sistema.

Com respeito à confidencialidade, pode-se resumir as duas asserções acima como a seguinte sentença (BIEBER; CUPPENS, 1992):

Se B sabe que φ então B tem a permissão para saber que φ

Em termos da lógica proposicional, tem-se a fórmula

$$K_B\varphi \rightarrow R_B\varphi$$

onde os operadores modais K_B e R_B designam, respectivamente, "tem o conhecimento" e "tem a permissão para conhecer", já definidos e adotados nas lógicas modais em trabalhos anteriores (GLASGOW; MACEWEN; PANANGADEN, 1992; BIEBER; CUPPENS, 1992).

A **linguagem** para o tratamento do conhecimento consiste em um conjunto de indivíduos U enumerados de 1 a n, um conjunto de proposições primitivas Σ, e do operador modal K_i. Uma proposição da forma $K_i\phi$ significa que o indivíduo i sabe que a proposição ϕ é verdadeira.

A fim de estabeler-se inequivocamente a **semântica** dos modelos a serem construídos, usar-se-á a noção de estruturas de Kripke (WALLISER, 1992; GLASGOW; MACEWEN; PANANGADEN, 1992), considerando-se que os indivíduos percebem diversos mundos possíveis. Formalmente, um modelo é uma estrutura $\mathscr{M} = (S, \pi, \kappa_1, \cdots, \kappa_n)$ de Kripke, onde:

1. S é o conjunto dos mundos possíveis;
2. a relação κ_i para o sujeito i é uma relação de equivalência (ou seja, reflexiva, simétrica e transitiva). Diz-se que dois mundos são **indistinguíveis** para o sujeito i se eles pertencem à mesma classe de equivalência em κ_i;
3. uma fórmula é definida como sendo verdadeira ou falsa, mas não simultaneamente ambos (*tertium non datur* - princípio do terceiro excluído) em um mundo possível. Escreve-se $s \models \phi$ para indicar que a fórmula ϕ é verdadeira no mundo s. Se for o caso, pode-se escrever $(\mathscr{M}, s) \models \phi$ para indicar que ϕ é verdadeira no mundo s sob o modelo $\mathscr{M}$;
4. para cada mundo $s \in S$ e para cada fórmula primitiva $\phi \in \Sigma$, π atribui um valor de verdade a ϕ em s (ou seja, $\pi(s, \phi) \in \{verdadeiro, falso\}$).

As condições mediante as quais uma fórmula assume o valor de verdade *verdadeiro* são as seguintes, sendo ϕ e ψ fórmulas:

1.para todas as $\phi \in \Sigma, s \models \phi$ sse (se e somente se) $\pi(s,\phi) = verdadeiro$;

2.$s \models \phi \wedge \psi$ sse $s \models \phi$ e $s \models \psi$;

3.$s \models \neg\phi$ sse não $s \models \phi$;

4.$s \models K_i\phi$ sse para todo s' tal que $(s,s') \in \kappa_i, s' \models \phi$.

Uma fórmula ϕ é dita **válida** em M (denotado por $M \models p$) se ela é verdadeira em todos os mundos $s \in S$. Denota-se isto por $\models \phi$.

Uma fórmula ϕ é dita **satisfatível** em $\mathscr{M}$ se $\neg\phi$ não é válida em $\mathscr{M}$.

Por sua vez, os axiomas definidos na lógica sobre o conhecimento são os seguintes (GLASGOW; MACEWEN; PANANGADEN, 1992):

1.*Axioma K1*. $K_i\phi \rightarrow \phi$. **Axioma do conhecimento**: um indivíduo não pode conhecer nada que seja falso - eis a distinção entre conhecimento e crença;

2.*Axioma K2*. $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$. **Axioma do fecho por conseqüência**: um indivíduo conhece todas as coisas que podem ser deduzidas a partir de seus conhecimentos. Esta dedução é feita por *modus ponens*: de $\models \phi$ e $\models \phi \rightarrow \psi$, deduz-se $\models \psi$;

3.*Axioma K3*. $K_i\phi \rightarrow K_i(K_i\phi)$. **Axioma da introspecção positiva**: um indivíduo conhece o seu próprio conhecimento.

4.*Axioma K4*. $\neg K_i\phi \rightarrow K_i(\neg K_i\phi)$. **Axioma da introspecção negativa**: um indivíduo conhece o seu próprio desconhecimento.

A teoria inclui todas as regras de prova da lógica proposicional (EPSTEIN, 1990, 1994), além de introduzir-se a **regra do conhecimento** de fórmulas válidas:

Regra C.1*Se ϕ é válida então $K_i\phi$.*

Ou seja, se a fórmula ϕ é válida (verdadeira em todos os mundos possíveis), então algum indivíduo a conhece.

C.2.2 Conhecimento e tempo

Glasgow, MacEwen e Panangaden (1992) apresentam uma lógica temporal para o conhecimento baseada em Ben-Ari, Manna e Pnueli (1981), na qual o modelo consiste em uma árvore cujos ramos denotam as alternativas temporais a partir de um mundo inicial s. Ao percorrimento dos ramos, estão associados os três operadores temporais, a saber, $\forall\Box$ (sempre), $\forall\Diamond$ (eventualmente [2]) e $\exists\Diamond$ (às vezes [3]), que correspondem aos quantificadores, definidos de tal modo que, dados um mundo s, um ramo definido como uma seqüência de mundos e uma fórmula ϕ, tem-se:

1. $s \models \forall\Box\phi$ sse ϕ é verdadeira em todos os mundos ao longo de todos os ramos iniciados em s;
2. $s \models \forall\Diamond\phi$ sse ϕ é verdadeira em algum mundo ao longo de todos os ramos iniciados em s;
3. $s \models \exists\Diamond\phi$ sse ϕ é verdadeira em algum mundo ao longo de algum ramo iniciado em s.

Além disso, dado um conjunto S de mundos possíveis, os elementos deste conjunto são chamados **"estados"**, indicando as configurações possíveis do sistema. Tem-se um conjunto $\mathscr{R}$ (finito ou infinito) de seqüências de membros de S chamados **execuções**. Se r é um membro de $\mathscr{R}$, escreve-se $r[i]$ para indicar o i-ésimo membro da seqüência r. Define-se então uma relação binária R entre os estados possíveis de S a partir do conjunto de execuções $\mathscr{R}$: para dois estados quaisquer s e s' de S, o par $(s,s') \in R$ se e somente se existe uma execução r tal que dados os inteiros i e j , $r[i] = s$ e $r[i+j] = s'$, ou seja, pode-se atingir s' a partir de s em um tempo finito.

De modo mais formal, o alfabeto desta linguagem consiste de:

1. um conjunto enumerável Σ de letras proposicionais primitivas $\phi, \psi, \ldots$;
2. os símbolos lógicos T (verdade) e $\bot$ (falsidade), e os conectivos lógicos $\neg$ (negação), $\wedge$ (conjunção), $\vee$ (disjunção) e $\rightarrow$ (implicação);
3. os operadores modais K_i (conhecimento) para todos os indivíduos; e
4. os operadores temporais $\forall\Box$ (sempre), $\forall\Diamond$ (eventualmente) e $\exists\Diamond$ (às vezes).

O conjunto de fórmulas bem-formadas da linguagem é o menor conjunto W tal que

[2] em Glasgow, MacEwen e Panangaden (1992), *eventually*.
[3] em Glasgow, MacEwen e Panangaden (1992), *sometimes*.

1.toda letra proposicional em Σ, assim como T e $\bot$, estão em W;

2.se ϕ e $\psi \in W$, então $\neg\phi$, $\phi \wedge \psi$, $\phi \vee \psi$, $\phi \rightarrow \psi$ e (ϕ) também $\in W$; e

3.se $\phi \in W$, então $K_i\phi$ (para todos os indivíduos i), $\forall\Box\phi$, $\forall\Diamond\phi$ e $\exists\Diamond\phi$ também $\in W$.

A semântica desta lógica temporal do conhecimento é a seguinte:

1.$s \models \forall\Box\phi$ sse para todos $(s,s') \in R, s' \models \phi$;

2.$s \models \forall\Diamond\phi$ sse para todo r, se $r[i] = s$, então existe s' e um inteiro não negativo j tal que $s' = r[i+j]$ e $s' \models \phi$;

3.$s \models \exists\Diamond\phi$ sse para algum $(s,s') \in R, s' \models \phi$.

Aos axiomas e regras da lógica do conhecimento, acrescentam-se ainda os seguintes axiomas (lembrando que $\exists\Diamond\phi \leftrightarrow \neg\forall\Box\neg\phi$):

1.*Axioma T1*. $\phi \rightarrow \forall\Diamond\phi$;

2.*Axioma T2*. $\forall\Box(\phi \rightarrow \psi) \rightarrow (\forall\Box\phi \rightarrow \forall\Box\psi$;

3.*Axioma T3*. $\forall\Box\phi \rightarrow \forall\Box\forall\Box\phi$.

As regras de inferência para a lógica temporal do conhecimento incluem a regra C.1, *modus ponens* e a seguinte **regra de generalização**:

Regra C.2*Se ϕ é válida então $\forall\Box\phi$ também o é.*

C.2.3 Permissão e obrigação

O alfabeto fornecido anteriormente é extendido com a inclusão de dois novos operadores modais: P (permissão) e O (obrigação) (GLASGOW; MACEWEN; PANANGADEN, 1992).

Além disso, o conjunto de fórmulas da linguagem é também extendido como se segue:

$\forall$ i, se $\phi \in W$ então $OK_i\phi, PK_i\phi, O\neg K_i\phi$ e $P\neg K_i\phi$ também $\in W$.

Os operadores deônticos P e O são duais no sentido modal: pode-se escrever um em termos do outro, como $P\phi \leftrightarrow \neg O\neg\phi$. Por conveniência, pode-se ainda escrever a fórmulas OK_i e PK_i como O_i e P_i, respectivamente.

A inclusão destes operadores permite a definição, em termos lógicos, das seguintes propriedades da segurança da informação:

1. **Propriedade do sigilo**: se $s \models K_i\phi$ então $s \models P_i\phi$; se um indíviduo sabe uma fórmula, então ele deve ter a permissão para sabê-la; inversamente, um indivóduo não deve conhecer fórmulas para as quais não a permissão de conhecer;

2. **Propriedade da integridade**: se $s \models O_i\phi$ então $s \models \forall\Diamond K_i\phi$; se um indivíduo é obrigado a conhecer uma fórmula, então eventualmente ele a conhecerá;

3. **Propriedade da acessibilidade**: para um sujeito i, estado s e fórmula ϕ quaisquer, se $s \models P_i\phi$ então $s \models \exists\Diamond K_i\phi$; se um indivíduo tem a permissão de conhecer uma fórmula, então ele pode vir a conhecê-la;

4. **Propriedade da obrigação**: para um sujeito i, estado s e fórmula ϕ quaisquer, se $s \models \forall\Box K_i\phi$, então $s \models O_i\phi$; se um indivíduo tem o conhecimento permanente de uma fórmula, então ele é obrigado a conhecê-la.

Os axiomas da linguagem extendida incluem os axiomas do conhecimento ($K1$ a $K4$) e da lógica temporal ($T1$ a $T3$) mostrados anteriormente, além da inclusão dos seguintes axiomas para as relações entre permissão e obrigatoriedade:

1. *Axioma SL1*. $P_i\phi$ para todas as tautologias proposionais ϕ;

2. *Axioma SL2*. $P_i\phi \rightarrow \phi$;

3. *Axioma SL3*. $(P_i\phi \wedge P_i\psi) \leftrightarrow P_i(\phi \wedge \psi)$;

4. *Axioma SL4*. $P_i\phi \rightarrow P(\phi \vee \psi)$;

5. *Axioma SL5*. $O_i\phi \rightarrow P_i\phi$.

Pelos axiomas acima, tem-se que a um indivíduo é permitido conhecer todas as tautologias proposicionais (SL1). Ainda, que toda fórmula permitida deve ser verdadeira (SL2), que a permissão se aplica por conjunção e por disjunção (SL3 e SL4) e que qualquer fórmula cujo conhecimento é obrigatório deve ser também permitida.

Glasgow, MacEwen e Panangaden (1992) apresentam ainda o teorema pelo qual os axiomas SL1 a SL5 são completos (*sound*) com respeito à semântica apresentada, e definem dois conjuntos, a saber, Θ_i é o conjunto das fórmulas que, se verdadeiras, o indivíduo i é obrigado a

conhecer, e Φ_i é o conjunto das fórmulas que, se verdadeiras, o indivíduo i tem a permissão para conhecer. As fórmulas nestes dois conjuntos podem ser das modalidades deôntica, epistêmica e temporal. Deste modo, para os autores, uma **política de segurança** é dada pela definição de propriedades dos conjuntos Θ_i e Φ_i. Uma **instância** de uma política de segurança é uma interpretação (uma atribuição de valores verdadeiro e falso) de um modelo para a lógica SL.

Uma instância é dita **correta** com respeito a uma política se ela é um modelo para SL e satisfaz as propriedades da política. Ainda, se dois sistemas que isoladamente obedecem a uma mesma política são interligados, e o sistema resultante ainda obedece à política, diz-se que esta política é **componível** (*composable*). De outro modo, se dois sistemas que independentemente obedecem a políticas distintas são interligados, e se a política resultante contém as duas políticas originais, estas são distas **compatíveis** (*compatible*).

Índice Remissivo